NETGEAR®

ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

Reference Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

July 29, 2011
202-10536-02
1.0

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, get support online, or for more information about the topics covered in this manual, visit the Support website at *http://support.netgear.com.*

Phone (US & Canada only): 1-888-NETGEAR

Phone (Other Countries): Check the list of phone numbers at *http://support.netgear.com/app/answers/detail/a_id/984*.

Trademarks

NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice. Other brand and product names are registered trademarks or trademarks of their respective holders. © 2011 NETGEAR, Inc. All rights reserved.

Statement of Conditions

To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

Revision History

Publication Part Number	Version	Publish Date	Comments
202-10536-02	1.0	July 2011	Added new features that are documented in the following sections: • *Configure WAN QoS Profiles* • *Inbound Rules (Port Forwarding)* and *LAN WAN Inbound Services Rules* • *Attack Checks* • *Set Session Limits* • *Create IP Groups* • *Use the NETGEAR VPN Client Wizard to Create a Secure Connection* • *Manually Create a Secure Connection Using the NETGEAR VPN Client* • *Configure the NETGEAR VPN Client for Mode Config Operation* • *Configure Date and Time Service* • *Enable the LAN Traffic Meter*
202-10536-01	1.0	April 2010	Initial publication of this reference manual.

Contents

Chapter 1 Introduction

Chapter 2 Connecting the VPN Firewall to the Internet

Chapter 3 LAN Configuration

Chapter 4 Firewall Protection

Chapter 5 Virtual Private Networking Using IPSec Connections

Chapter 6 Virtual Private Networking Using SSL Connections

Appendix D Two-Factor Authentication

Appendix E Notification of Compliance

Index

Introduction

1

This chapter provides an overview of the features and capabilities of the ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308. This chapter contains the following sections:

What Is the ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308?

The ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308, hereafter referred to as the VPN firewall, connects your local area network (LAN) to the Internet through up to four external broadband access devices such as cable modems or DSL modems. Four wide area network (WAN) ports allow you to increase effective data rate to the Internet by utilizing all WAN ports to carry session traffic or to maintain backup connections in case of failure of your primary Internet connection.

The VPN firewall is a complete security solution that protects your network from attacks and intrusions. For example, the VPN firewall provides support for stateful packet inspection (SPI), denial of service (DoS) attack protection, and multi-NAT support. The VPN firewall supports multiple web content filtering options, plus browsing activity reporting and instant alerts—both via email. Network administrators can establish restricted access policies based on time of day, website addresses, and address keywords.

The VPN firewall provides advanced IPSec and SSL VPN technologies for secure and simple remote connections. The use of Gigabit Ethernet LAN and WAN ports ensures extremely high data transfer speeds.

The VPN firewall is a plug-and-play device that can be installed and configured within minutes.

Key Features and Capabilities

The VPN firewall provides the following key features and capabilities:

- Four 10/100/1000 Mbps Gigabit Ethernet WAN ports for load balancing and failover protection of your Internet connection, providing increased data rate and increased system reliability.
- Built-in four-port 10/100/1000 Mbps Gigabit Ethernet LAN switch for extremely fast data transfer between local network resources and support for up to 200,000 internal or external connections.
- Advanced IPSec VPN and SSL VPN support with support for up to 125 concurrent IPSec VPN tunnels and up to 50 concurrent SSL VPN tunnels.
- Bundled with a single-user license of the NETGEAR ProSafe VPN Client software (VPN01L).
- Advanced stateful packet inspection (SPI) firewall with multi-NAT support.
- Quality of service (QoS) and SIP 2.0 support for traffic prioritization, voice, and multimedia.
- Extensive protocol support.
- Easy, web-based wizard setup for installation and management.
- One console port for local management.
- SNMP-manageable, optimized for the NETGEAR ProSafe Network Management Software (NMS100).
- Front panel LEDs for easy monitoring of status and activity.
- Flash memory for firmware upgrade.
- Internal universal switching power supply.
- One U rack-mountable, using the rack-mounting kit.

Quad-WAN Ports for Increased Reliability and Outbound Load Balancing

The VPN firewall provides four broadband WAN ports. These WAN ports allow you to connect additional broadband Internet lines that can be configured to:

- Load-balance between up to four lines for maximum bandwidth efficiency.
- Provide backup and rollover if one line is inoperable, ensuring that you are never disconnected.

See *Network Planning for Multiple WAN Ports* on page 306 for the planning factors to consider when implementing the following capabilities with multiple WAN port gateways:

- Single or multiple exposed hosts.
- Virtual private networks (VPNs).

Advanced VPN Support for Both IPSec and SSL

The VPN firewall supports IPSec and SSL VPN connections.

- IPSec VPN delivers full network access between a central office and branch offices, or between a central office and telecommuters. Remote access by telecommuters requires the installation of VPN client software on the remote computer.
  - IPSec VPN with broad protocol support for secure connection to other IPSec gateways and clients.
  - Bundled with a single-user license of the NETGEAR ProSafe VPN Client software (VPN01L).
  - Supports 125 concurrent IPSec VPN tunnels.
- SSL VPN provides remote access for mobile users to selected corporate resources without requiring a pre-installed VPN client on their computers.
  - Uses the familiar Secure Sockets Layer (SSL) protocol, commonly used for e-commerce transactions, to provide client-free access with customizable user portals and support for a wide variety of user repositories.
  - Browser-based, platform-independent, remote access through a number of popular browsers, such as Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari.
  - Provides granular access to corporate resources based on user type or group membership.
  - Supports 50 concurrent SSL VPN sessions.

A Powerful, True Firewall with Content Filtering

Unlike simple NAT routers, the VPN firewall is a true firewall, using stateful packet inspection (SPI) to defend against hacker attacks. Its firewall features have the following capabilities:

- **DoS protection**. Automatically detects and thwarts denial of service (DoS) attacks such as Ping of Death and SYN flood.
- **Secure firewall**. Blocks unwanted traffic from the Internet to your LAN.
- **Content filtering**. Prevents objectionable content from reaching your PCs. You can control access to Internet content by screening for web services, web addresses, and keywords within web addresses. You can configure the VPN firewall to log and report attempts to access objectionable Internet sites.
- **Schedule policies**. Permits scheduling of firewall policies by day and time.
- **Logs security incidents**. Logs security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the VPN firewall to email the log to you at specified intervals. You can also configure the VPN firewall to send immediate alert messages to your email address or email pager when a significant event occurs.

Security Features

The VPN firewall is equipped with several features designed to maintain security:

- **PCs hidden by NAT**. NAT opens a temporary path to the Internet for requests originating from the local network. Requests originating from outside the LAN are discarded, preventing users outside the LAN from finding and directly accessing the computers on the LAN.
- **Port forwarding with NAT**. Although NAT prevents Internet locations from directly accessing the PCs on the LAN, the VPN firewall allows you to direct incoming traffic to specific PCs based on the service port number of the incoming request. You can specify forwarding of single ports or ranges of ports.
- **DMZ port**. Incoming traffic from the Internet is normally discarded by the VPN firewall unless the traffic is a response to one of your local computers or a service for which you have configured an inbound rule. Instead of discarding this traffic, you can use the dedicated demilitarized zone (DMZ) port to forward the traffic to one PC on your network.

Autosensing Ethernet Connections with Auto Uplink

With its internal four-port 10/100/1000 Mbps switch and four 10/100/1000 WAN ports, the VPN firewall can connect to either a 10 Mbps standard Ethernet network, a 100 Mbps Fast Ethernet network, or a 1000 Mbps Gigabit Ethernet network. The four LAN and four WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

The VPN firewall incorporates Auto UplinkTM technology. Each Ethernet port automatically senses whether the Ethernet cable plugged into the port should have a normal connection such as to a PC or an uplink connection such as to a switch or hub. That port then configures itself correctly. This feature eliminates the need for you to think about crossover cables, as Auto Uplink accommodates either type of cable to make the right connection.

Extensive Protocol Support

The VPN firewall supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). For further information about TCP/IP, see *Internet Configuration Requirements* on page 308. The VPN firewall provides the following protocol support:

- **IP address sharing by NAT**. The VPN firewall allows many networked PCs to share an Internet account using only a single IP address, which might be statically or dynamically assigned by your Internet Service Provider (ISP). This technique, known as NAT, allows the use of an inexpensive single-user ISP account.
- **Automatic configuration of attached PCs by DHCP**. The VPN firewall dynamically assigns network configuration information, including IP, gateway, and Domain Name Server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of PCs on your local network.

- **DNS proxy**. When DHCP is enabled and no DNS addresses are specified, the VPN firewall provides its own address as a DNS server to the attached PCs. The VPN firewall obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.
- **PPP over Ethernet (PPPoE)**. PPPoE is a protocol for connecting remote hosts to the Internet over a DSL connection by simulating a dial-up connection. This feature eliminates the need to run a login program.
- **Quality of Service (QoS)**. The VPN firewall supports QoS, including traffic prioritization and traffic classification with Type of Service (ToS) and Differentiated Services Code Point (DSCP) marking.

Easy Installation and Management

You can install, configure, and operate the VPN firewall within minutes after connecting it to the network. The following features simplify installation and management tasks:

- **Browser-based management**. Browser-based configuration allows you to easily configure the VPN firewall from almost any type of operating system, such as Windows, Macintosh, or Linux. Online help documentation is built into the browser-based web management interface.
- **Auto detection of ISP**. The VPN firewall automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- **IPSec VPN Wizard**. The VPN firewall includes the NETGEAR IPSec VPN Wizard so you can easily configure IPSec VPN tunnels according to the recommendations of the Virtual Private Network Consortium (VPNC) to ensure that the IPSec VPN tunnels are interoperable with other VPNC-compliant VPN routers and clients.
- **SNMP**. The VPN firewall supports the Simple Network Management Protocol (SNMP) to let you monitor and manage log resources from an SNMP-compliant system manager. The SNMP system configuration lets you change the system variables for MIB2.
- **Diagnostic functions**. The VPN firewalll incorporates built-in diagnostic functions such as ping, traceroute, DNS lookup, and remote reboot.
- **Remote management**. The VPN firewall allows you to log in to the web management interface from a remote location on the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses.
- **Visual monitoring**. The VPN firewall’s front panel LEDs provide an easy way to monitor its status and activity.

Maintenance and Support

NETGEAR offers the following features to help you maximize your use of the VPN firewall:

- Flash memory for firmware upgrades.
- Technical support seven days a week, 24 hours a day, according to the terms that are identified in the Warranty and Support information card provided with your product.

Package Contents

The VPN firewall product package contains the following items:

- ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308 appliance
- One AC power cable
- Rubber feet (4)
- One Category 5 (Cat5) Ethernet cable
- One rack-mounting kit
- *ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308 Installation Guide*
- *Resource CD*, including:
  - Application Notes and other helpful information
  - ProSafe VPN Client software (VPN01L)

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the product for repair.

Hardware Features

The front panel ports and LEDs, rear panel ports, and bottom label of the VPN firewall are described in the following sections.

Front Panel

Viewed from left to right, the VPN firewall front panel contains the following ports (see the following figure).

- LAN Ethernet ports: four switched N-way automatic speed negotiating, Auto MDI/MDIX, Gigabit Ethernet ports with RJ-45 connectors
- WAN Ethernet ports: four independent N-way automatic speed negotiating, Auto MDI/MDIX, Gigabit Ethernet ports with RJ-45 connectors

The front panel also contains three groups of status indicator light-emitting diodes (LEDs), including Power and Test LEDs, LAN LEDs, and WAN LEDs, all of which are explained in the following table.

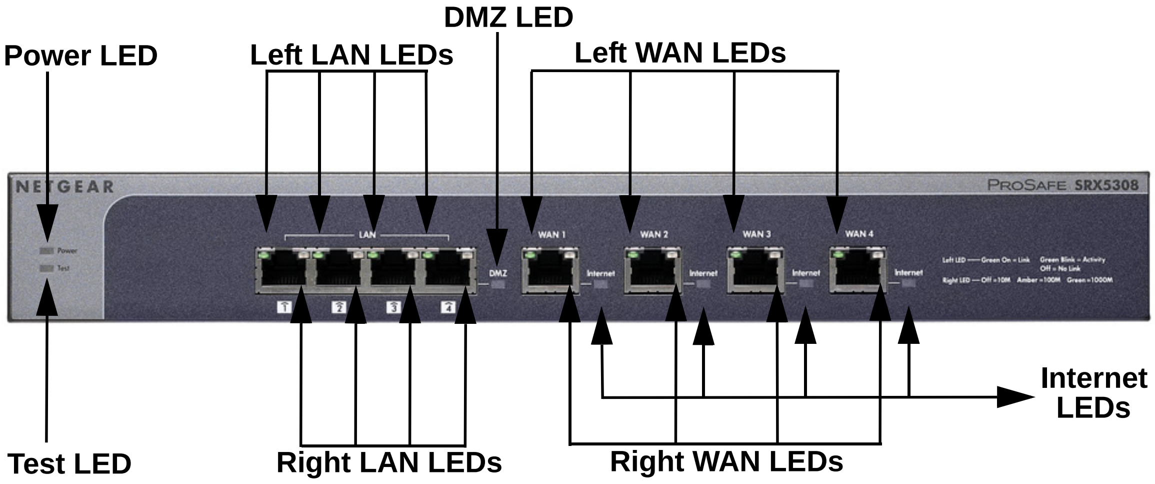


Figure 1.

Table 1. LED descriptions

LED	Activity	Description
Power	On (green)	Power is supplied to the VPN firewall.
	Off	Power is not supplied to the VPN firewall.
Test	On (amber) during startup.	Test mode: the VPN firewall is initializing. After approximately 2 minutes, when the VPN firewall has completed its initialization, the Test LED goes off.
	On (amber) during any other time	The initialization has failed or a hardware failure has occurred.
	Blinking (amber)	The VPN firewall is writing to flash memory (during upgrading or resetting to defaults).
	Off	The system has booted successfully.
LAN Ports		
Left LED	On (green)	The LAN port has detected a link with a connected Ethernet device.
	Blinking (green)	Data is being transmitted or received by the LAN port.
	Off	The LAN port has no link.
Right LED	On (green)	The LAN port is operating at 1000 Mbps.
	On (amber)	The LAN port is operating at 100 Mbps.
	Off	The LAN port is operating at 10 Mbps.
DMZ LED	On (green)	Port 4 is operating as a dedicated hardware DMZ port.
	Off	Port 4 is operating as a normal LAN port.

Table 1. LED descriptions (continued)

LED	Activity	Description
WAN Ports		
Left LED	On (green)	The WAN port has a valid connection with a device that provides an Internet connection.
	Blinking (green)	Data is being transmitted or received by the WAN port.
	Off	The WAN port has no physical link, that is, no Ethernet cable is plugged into the VPN firewall.
Right LED	On (green)	The WAN port is operating at 1000 Mbps.
	On (amber)	The WAN port is operating at 100 Mbps.
	Off	The WAN port is operating at 10 Mbps.
Internet LED	On (green)	The WAN port has a valid Internet connection.
	Off	The WAN port is either not enabled or has no link to the Internet.

Rear Panel

The rear panel of the VPN firewall includes a console port, a reset button, a cable lock receptacle, an AC power connection, and a power switch.

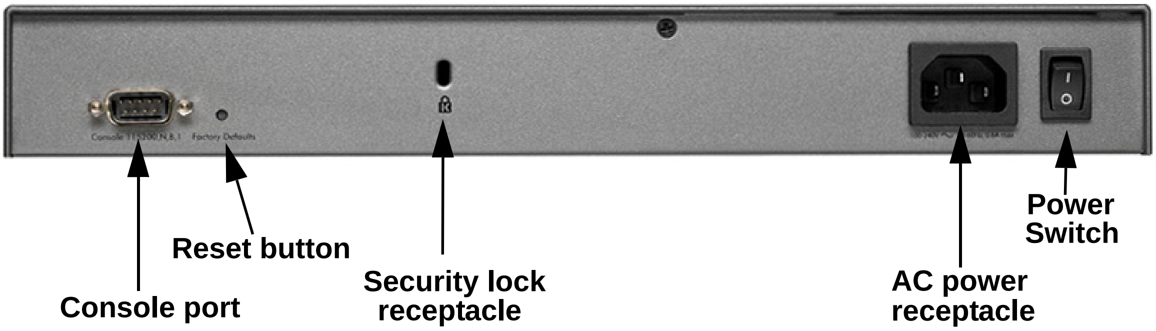


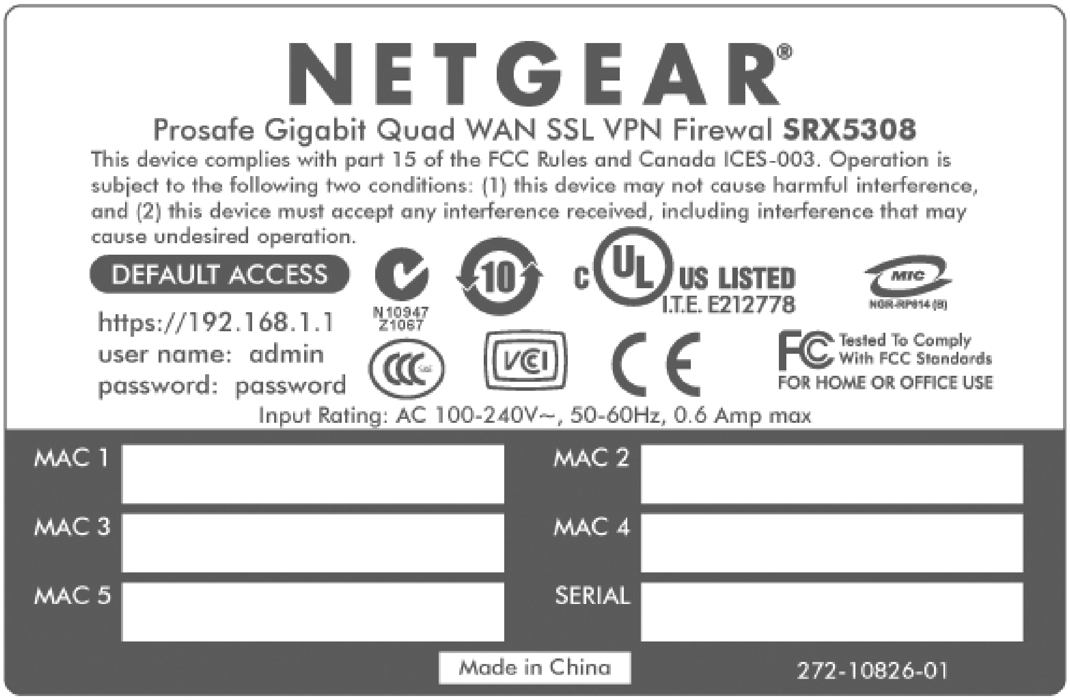
Figure 2.

Viewed from left to right, the rear panel contains the following components:

1. Cable security lock receptacle.
2. Console port. Port for connecting to an optional console terminal. The ports has a DB9 male connector. The default baud rate is 9600 K. The pinouts are: (2) Tx, (3) Rx, (5) and (7) Gnd. For information about accessing the command line interface (CLI) using the console port, see *Using the Command-Line Interface* on page 253.
3. Factory default reset button. Using a sharp object, press and hold this button for about eight seconds until the front panel Test light flashes to reset the VPN firewall to factory default settings. All configuration settings are lost, and the default password is restored.
4. AC power receptacle. Universal AC input (100–240 VAC, 50–60 Hz).
5. A power on/off switch.

Bottom Panel with Product Label

The product label on the bottom of the VPN firewall's enclosure displays factory default settings, regulatory compliance, and other information.



NETGEAR®

Prosafe Gigabit Quad WAN SSL VPN Firewal **SRX5308**

This device complies with part 15 of the FCC Rules and Canada ICES-003. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

DEFAULT ACCESS

https://192.168.1.1
user name: admin
password: password

N10947
Z1067

c UL US LISTED
I.T.E. E212778

Tested To Comply With FCC Standards
FOR HOME OR OFFICE USE

Input Rating: AC 100-240V~, 50-60Hz, 0.6 Amp max

MAC 1		MAC 2	
MAC 3		MAC 4	
MAC 5		SERIAL	

Made in China

272-10826-01

Figure 3.

Choose a Location for the VPN Firewall

The VPN firewall is suitable for use in an office environment where it can be free-standing (on its runner feet) or mounted into a standard 19-inch equipment rack. Alternatively, you can rack-mount the VPN firewall in a wiring closet or equipment room. A rack-mounting kit, containing two mounting brackets and four screws, is provided in the package.

Consider the following when deciding where to position the VPN firewall:

- The unit is accessible and cables can be connected easily.
- Cabling is away from sources of electrical noise. These include lift shafts, microwave ovens, and air-conditioning units.
- Water or moisture cannot enter the case of the unit.
- Airflow around the unit and through the vents in the side of the case is not restricted. Provide a minimum of 25 mm or 1 inch clearance.
- The air is as free of dust as possible.
- Temperature operating limits are not likely to be exceeded. Install the unit in a clean, air-conditioned environment. For information about the recommended operating temperatures for the VPN firewall, see *Appendix A, Default Settings and Technical Specifications*.

Using the Rack-Mounting Kit

Use the mounting kit for the VPN firewall to install the appliance in a rack. Attach the mounting brackets using the hardware that is supplied with the mounting kit.

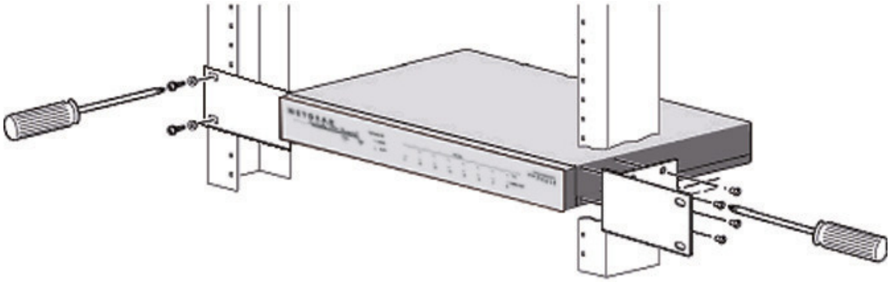


Figure 4.

Before mounting the VPN firewall in a rack, verify that:

- You have the correct screws (supplied with the installation kit).
- The rack onto which you will mount the VPN firewall is suitably located.

Connecting the VPN Firewall to the Internet

2

This chapter contains the following sections:

- *Internet and WAN Configuration Tasks*
- *Log In to the VPN Firewall*
- *Configure the Internet Connections*
- *Configure the WAN Mode*
- *Configure Secondary WAN Addresses*
- *Configure Dynamic DNS*
- *Configure WAN QoS Profiles*
- *Configure Advanced WAN Options*
- *What to Do Next*

Internet and WAN Configuration Tasks

Typically, the VPN firewall is installed as a network gateway to function as a combined LAN switch and firewall in order to protect the network from incoming threats and provide secure connections. To complement the firewall protection, NETGEAR advises that you use a gateway security appliance such as a NETGEAR ProSecure STM appliance.

➢ **Generally, seven steps are required to complete the Internet connection of your VPN firewall:**

1. **Connect the VPN firewall physically to your network**. Connect the cables and restart your network according to the instructions in the installation guide. See the *ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308 Installation Guide* for complete steps. A PDF of the *Installation Guide* is on the NETGEAR website at *http://support.netgear.com/app/products/model/a_id/13568*.
2. **Log in to the VPN firewall**. After logging in, you are ready to set up and configure your VPN firewall. See *Log In to the VPN Firewall* on page 20.
3. **Configure the Internet connections to your ISPs**. During this phase, you connect to your ISPs. You can also program the WAN traffic meters at this time if desired. See *Configure the Internet Connections* on page 24.

4. **Configure the WAN mode.** Select either NAT or classical routing. Select load balancing mode, auto-rollover mode, or primary (single) WAN mode. For load balancing, you can also select any necessary protocol bindings. See *Configure the WAN Mode* on page 32.
5. **Configure secondary WAN addresses on the WAN ports (optional)**. Configure aliases for each WAN port. See *Configure Secondary WAN Addresses* on page 41.
6. **Configure dynamic DNS on the WAN ports (optional)**. Configure your fully qualified domain names. See *Configure Dynamic DNS* on page 42.
7. **Configure the WAN options (optional)**. You can enable each WAN port to respond to a ping, and you can change the factory default MTU size and port speed. However, these are advanced features and changing them is not usually required. See *Configure Advanced WAN Options* on page 51.

Each of these tasks is detailed separately in this chapter.

Note: For information about how to configure the WAN meters, see *Enable the WAN Traffic Meter* on page 263.

The configuration of LAN, firewall, scanning, VPN, management, and monitoring features is described in later chapters.

Qualified Web Browsers

To configure the VPN firewall, you need to use a web browser such as Microsoft Internet Explorer 6 or later, Mozilla Firefox 3 or later, or Apple Safari 3 or later with JavaScript, cookies, and SSL enabled.

Although these web browsers are qualified for use with the VPN firewall's web management interface, SSL VPN users should choose a browser that supports JavaScript, Java, cookies, SSL, and ActiveX to take advantage of the full suite of applications. Note that Java is required only for the SSL VPN portal, not for the web management interface.

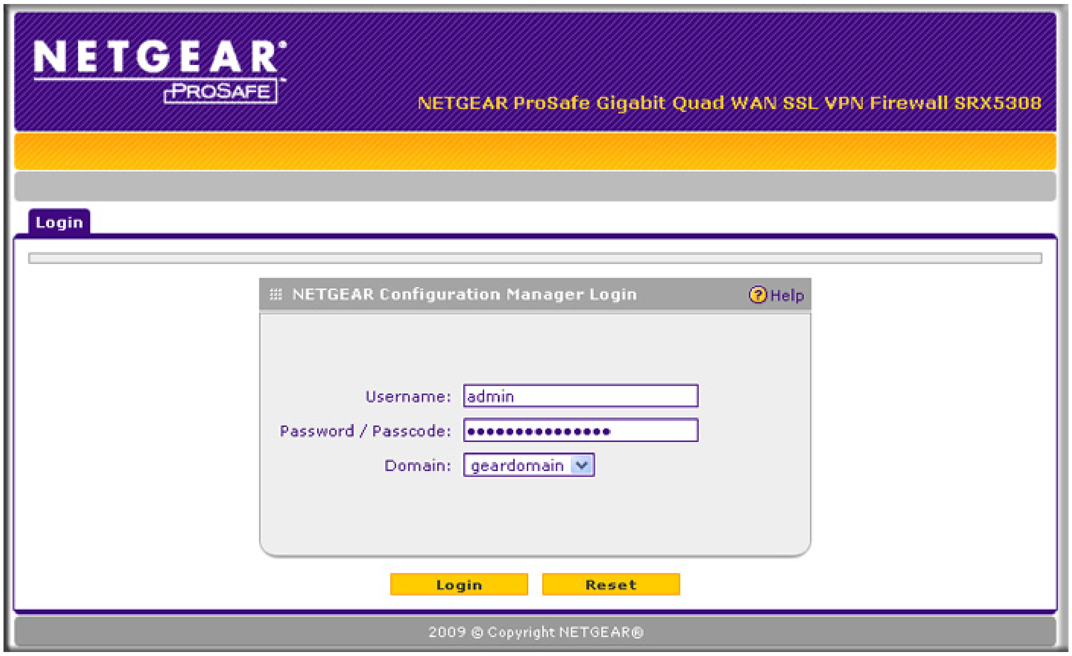
Log In to the VPN Firewall

To connect to the VPN firewall, your computer needs to be configured to obtain an IP address automatically from the VPN firewall via DHCP.

➢ **To connect and log in to the VPN firewall:**

1. Start any of the qualified web browsers, as explained in *Qualified Web Browsers* on page 20.
2. Enter **https://192.168.1.1** in the address field. The NETGEAR Configuration Manager Login screen displays in the browser.

Note: The VPN firewall factory default IP address is 192.168.1.1. If you change the IP address, you need to use the IP address that you assigned to the VPN firewall to log in to the VPN firewall.


NETGEAR ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308
Login
NETGEAR Configuration Manager Login
Help
Login
Reset
2009 © Copyright NETGEAR®

Username: admin

Password / Passcode: •••••••••••••••

Domain: geardomain

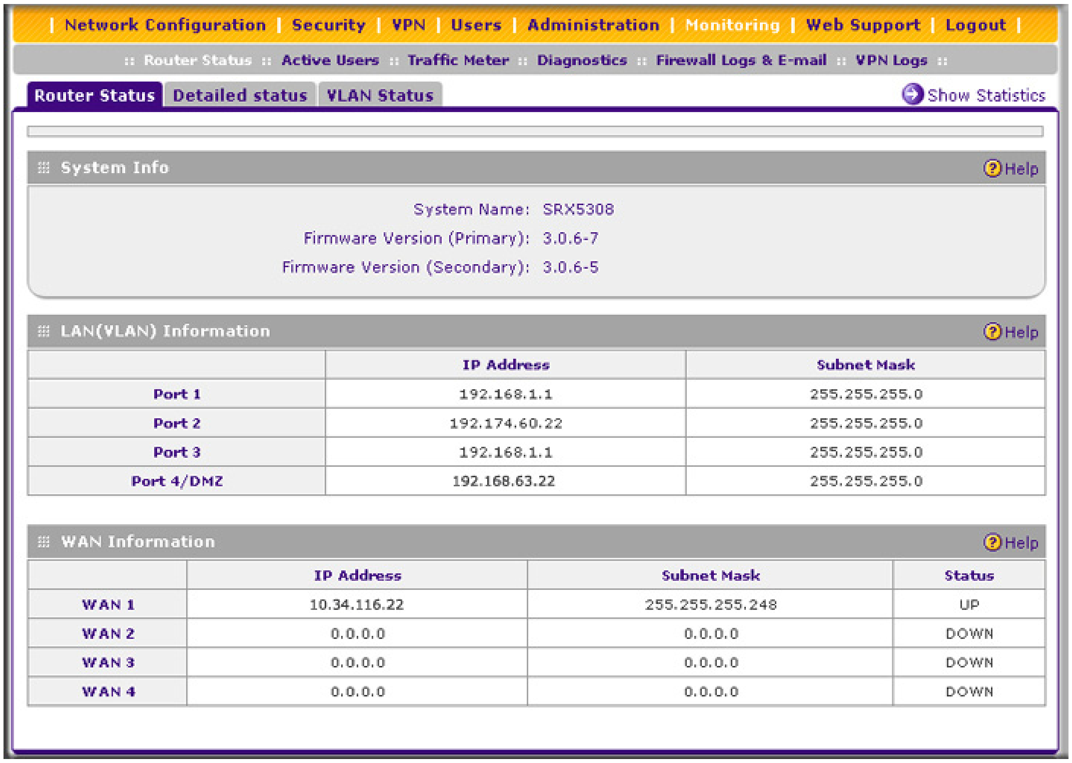
Figure 5.

Note: The first time that you remotely connect to the VPN firewall with a browser via an SSL connection, you might get a warning message regarding the SSL certificate. Follow the directions of your browser to accept the SSL certificate.

3. In the Username field, type **admin**. Use lower-case letters.
4. In the Password / Passcode field, type **password**. Here, too, use lower-case letters.

Note: The VPN firewall user name and password are not the same as any user name or password you might use to log in to your Internet connection.

5. In the **Domain** drop-down list, leave the default selection, which is geardomain.
6. Click **Login.** The web management interface appears, displaying the Router Status screen. (For information about this screen, see *View the System (Router) Status and Statistics* on page 275.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Router Status
Detailed status
VLAN Status
Show Statistics
Help
Help
Help

System Info

System Name: SRX5308
Firmware Version (Primary): 3.0.6-7
Firmware Version (Secondary): 3.0.6-5

LAN(VLAN) Information

	IP Address	Subnet Mask
Port 1	192.168.1.1	255.255.255.0
Port 2	192.174.60.22	255.255.255.0
Port 3	192.168.1.1	255.255.255.0
Port 4/DMZ	192.168.63.22	255.255.255.0

WAN Information

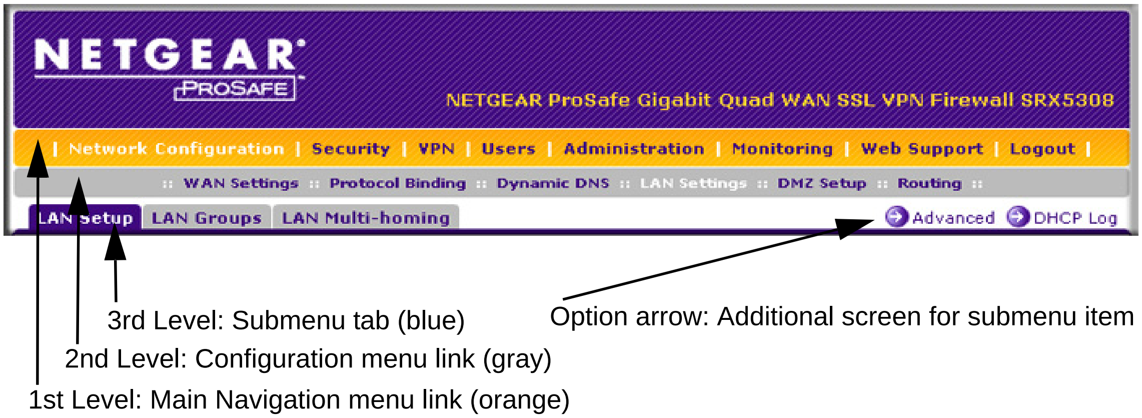
	IP Address	Subnet Mask	Status
WAN 1	10.34.116.22	255.255.255.248	UP
WAN 2	0.0.0.0	0.0.0.0	DOWN
WAN 3	0.0.0.0	0.0.0.0	DOWN
WAN 4	0.0.0.0	0.0.0.0	DOWN

Figure 6.

Note: After 10 minutes of inactivity (the default login time-out), you are automatically logged out.

Web Management Interface Menu Layout

The following figure shows the menu at the top of the web management interface.


NETGEAR
PROSAFE
NETGEAR ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308
| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing ::
LAN Setup
LAN Groups
LAN Multi-homing
Advanced
DHCP Log

3rd Level: Submenu tab (blue)

Option arrow: Additional screen for submenu item

2nd Level: Configuration menu link (gray)

1st Level: Main Navigation menu link (orange)

Figure 7.

The web management interface menu consists of the following components:

- **1st Level: main navigation menu links**. The main navigation menu in the orange bar across the top of the web management interface provides access to all the configuration functions of the VPN firewall, and remains constant. When you select a main navigation menu link, the letters are displayed in white against an orange background.
- **2nd Level: configuration menu links**. The configuration menu links in the gray bar (immediately below the main navigation menu bar) change according to the main navigation menu link that you select. When you select a configuration menu link, the letters are displayed in white against a gray background.
- **3rd Level: submenu tabs**. Each configuration menu item has one or more submenu tabs that are listed below the gray menu bar. When you select a submenu tab, the text is displayed in white against a blue background.
- **Option arrows**. If there are additional screens for the submenu item, they are displayed on the right side in blue letters against a white background, preceded by a white arrow in a blue circle.

The bottom of each screen provides action buttons. The nature of the screen determines which action buttons are shown. The following figure shows an example.

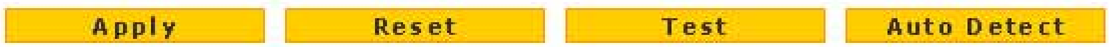


Figure 8.

Any of the following action buttons might be displayed on screen (this list might not be complete):

- **Apply**. Save and apply the configuration.
- **Reset**. Reset the configuration to default values.
- **Test**. Test the configuration before you decide whether or not to save and apply the configuration.

- **Auto Detect**. Enable the VPN firewall to detect the configuration automatically and suggest values for the configuration.
- **Next**. Go to the next screen (for wizards).
- **Back**. Go to the previous screen (for wizards).
- **Search**. Perform a search operation.
- **Cancel**. Cancel the operation.
- **Send Now**. Send a file or report.

When a screen includes a table, table buttons are displayed to let you configure the table entries. The nature of the screen determines which table buttons are shown. The following figure shows an example.

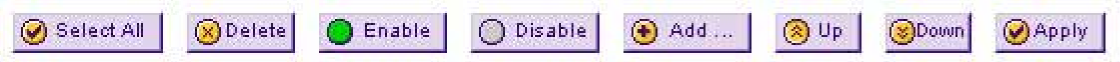


Figure 9.

Any of the following table buttons might be displayed on screen:

- **Select All**. Select all entries in the table.
- **Delete**. Delete the selected entry or entries from the table.
- **Enable**. Enable the selected entry or entries in the table.
- **Disable**. Disable the selected entry or entries in the table.
- **Add**. Add an entry to the table.
- **Edit**. Edit the selected entry.
- **Up**. Move up the selected entry in the table.
- **Down**. Move down the selected entry in the table.
- **Apply**. Apply the selected entry.

Almost all screens and sections of screens have an accompanying help screen. To open the help screen, click the **Help** icon (? Help).

Configure the Internet Connections

To set up your VPN firewall for secure Internet connections, you configure WAN ports 1 through 4. The web management interface offers two connection configuration options:

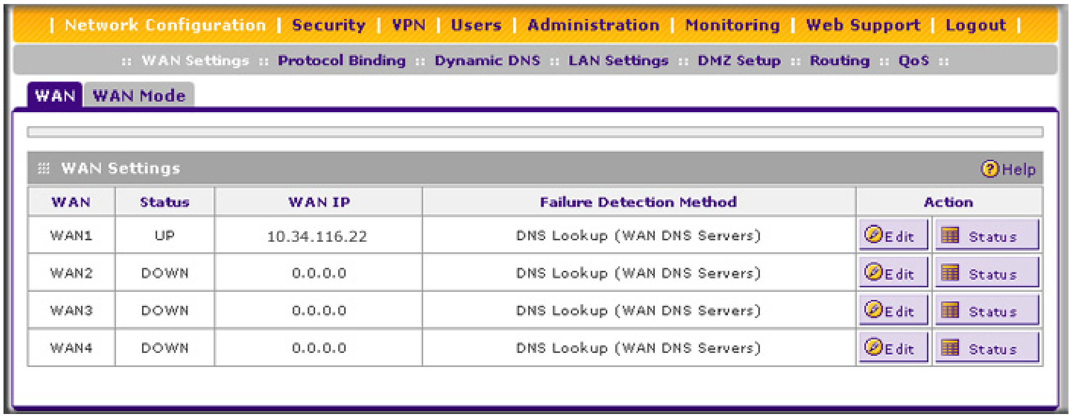
- Automatic detection and configuration of the network connection
- Manual configuration of the network connection

Each option is detailed in a section that follows.

Automatically Detecting and Connecting

➢ **To automatically configure the WAN ports for connection to the Internet:**

1. Select **Network Configuration > WAN Settings**. The WAN screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
WAN
WAN Mode
WAN Settings
Help

WAN	Status	WAN IP	Failure Detection Method	Action	
WAN1	UP	10.34.116.22	DNS Lookup (WAN DNS Servers)	Edit	Status
WAN2	DOWN	0.0.0.0	DNS Lookup (WAN DNS Servers)	Edit	Status
WAN3	DOWN	0.0.0.0	DNS Lookup (WAN DNS Servers)	Edit	Status
WAN4	DOWN	0.0.0.0	DNS Lookup (WAN DNS Servers)	Edit	Status

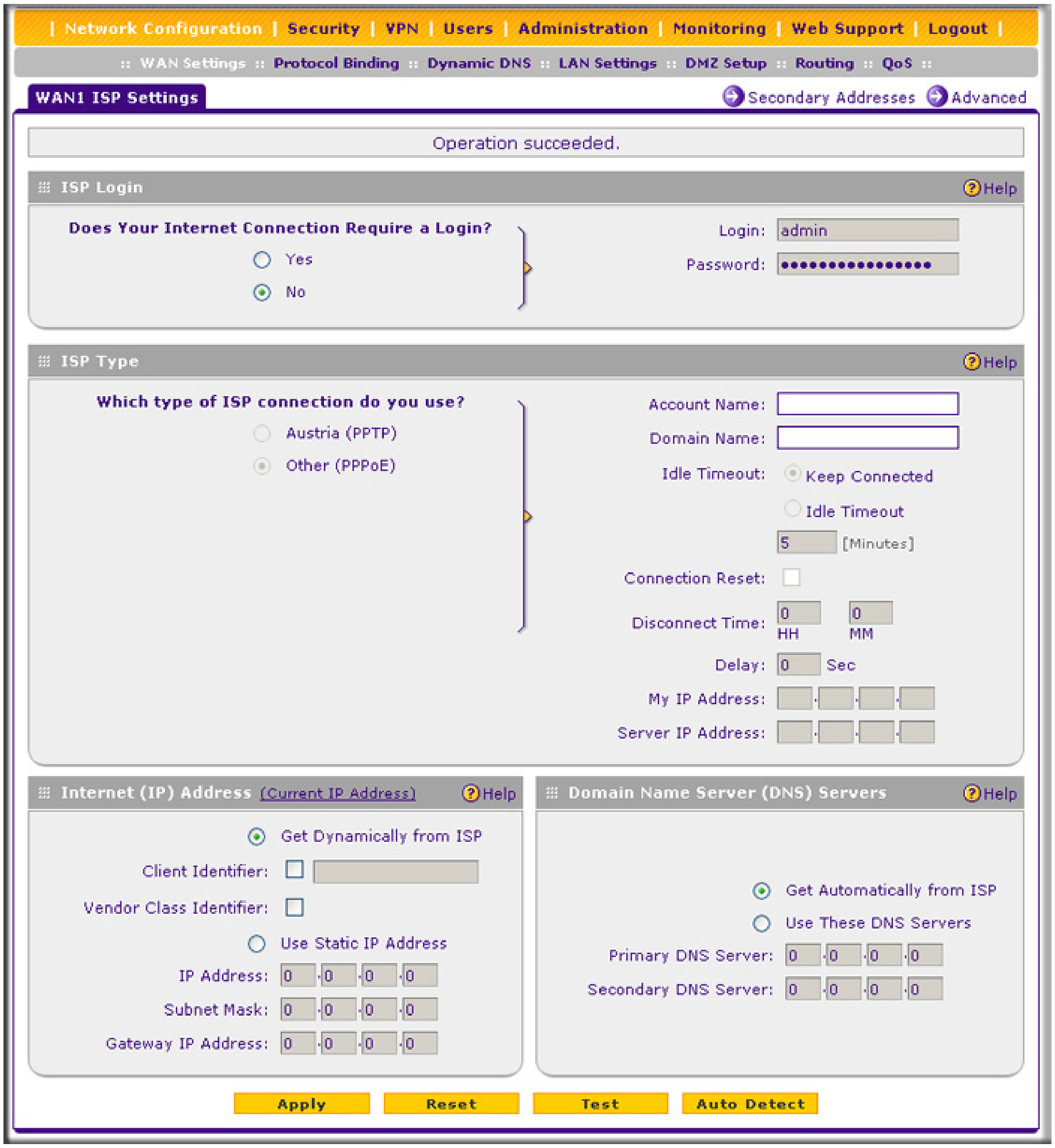
Figure 10.

The WAN Settings table displays the following fields:

- **WAN**. The WAN interface (WAN1, WAN2, WAN3, and WAN4).
- **Status**. The status of the WAN interface (UP or DOWN).
- **WAN IP**. The IP address of the WAN interface.
- **Failure Detection Method**. The failure detection method that is active for the WAN interface. The following methods can be displayed:
  - None
  - DNS Lookup (WAN DNS Server)
  - DNS Lookup (the configured IP address is displayed)
  - PING (the configured IP address is displayed)

  You can set the failure detection method for each WAN interface on its corresponding WAN Advanced Options screen (see *Configure the Auto-Rollover Mode and Failure Detection Method* on page 34).
- **Action**. The Edit table button provides access to the WAN ISP Settings screen (see *step 2*) for the corresponding WAN interface; the Status button provides access to the Connection Status screen (see *step 4*) for the corresponding WAN interface.

2. Click the **Edit** table button in the Action column of the WAN interface for which you want to automatically configure the connection to the Internet. The WAN ISP Settings screen displays. (The following figure shows the WAN1 ISP Settings screen as an example.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
Secondary Addresses
Advanced
Help
Apply
Reset
Test
Auto Detect

WAN1 ISP Settings

Operation succeeded.

ISP Login

Does Your Internet Connection Require a Login?

○ Yes

● No

Login: admin

Password: ••••••••••••••••

ISP Type

Which type of ISP connection do you use?

○ Austria (PPTP)

● Other (PPPoE)

Account Name:

Domain Name:

Idle Timeout: ● Keep Connected ○ Idle Timeout 5 [Minutes]

Connection Reset: □

Disconnect Time: 0 HH 0 MM

Delay: 0 Sec

My IP Address: . . .

Server IP Address: . . .

Internet (IP) Address (Current IP Address)

● Get Dynamically from ISP

Client Identifier: □

Vendor Class Identifier: □

○ Use Static IP Address

IP Address: 0 .0 .0 .0

Subnet Mask: 0 .0 .0 .0

Gateway IP Address: 0 .0 .0 .0

Domain Name Server (DNS) Servers

● Get Automatically from ISP

○ Use These DNS Servers

Primary DNS Server: 0 .0 .0 .0

Secondary DNS Server: 0 .0 .0 .0

Figure 11.

3. Click the **Auto Detect** button at the bottom of the screen. The auto detect process probes the WAN port for a range of connection methods and suggests one that your ISP is most likely to support.

   The auto detect process returns one of the following results:

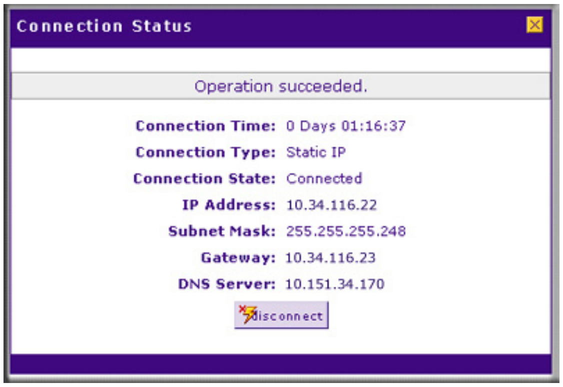
   - If the auto-detect process is successful, a status bar at the top of the screen displays the results (for example, *DHCP service detected*).
   - If the auto detect process senses a connection method that requires input from you, it prompts you for the information. All methods with their required settings are explained in the following table:

Table 2. Internet connection methods

Connection method	Manual data input required
DHCP (Dynamic IP)	No data is required.
PPPoE	Login, Password, Account Name, Domain Name
PPTP	Login, Password, Account Name, My IP Address, and Server IP Address.
Fixed (Static) IP	IP Address, Subnet Mask, and Gateway IP Address; and related data supplied by your ISP.

- If the auto detect process does not find a connection, you are prompted either to check the physical connection between your VPN firewall and the cable or DSL line or to check your VPN firewall's MAC address. For more information, see *Configure the WAN Mode* on page 32 and *Troubleshoot the ISP Connection* on page 296.

4. Verify the connection:
   a. Return to the WAN screen by selecting **Network Configuration > WAN Settings**.
   b. Click the **Status** button in the Action column of the WAN interface that you just configured to display the Connection Status popup window:



Connection Status

Operation succeeded.

Connection Time: 0 Days 01:16:37
Connection Type: Static IP
Connection State: Connected
IP Address: 10.34.116.22
Subnet Mask: 255.255.255.248
Gateway: 10.34.116.23
DNS Server: 10.151.34.170

Figure 12.

The WAN Status window should show a valid IP address and gateway. If the configuration was not successful, skip ahead to *Manually Configure the Internet Connection* on this page or see *Troubleshoot the ISP Connection* on page 296.

Note: If the configuration process was successful, you are connected to the Internet through the WAN interfaces that you just configured. Continue with the configuration process for the other WAN interfaces.

Note: For more information about the WAN Connection Status screen, see *View the WAN Port Connection Status* on page 285.

5. Repeat *step 2*, *step 3*, and *step 4* for the other WAN interfaces that you want to configure.

If your WAN ISP configuration was successful, you can skip ahead to *Configure the WAN Mode* on page 32.

If one or both automatic WAN ISP configurations failed, you can attempt a manual configuration as described in *Manually Configure the Internet Connection* on this page or see *Troubleshoot the ISP Connection* on page 296.

Set the VPN Firewall's MAC Address

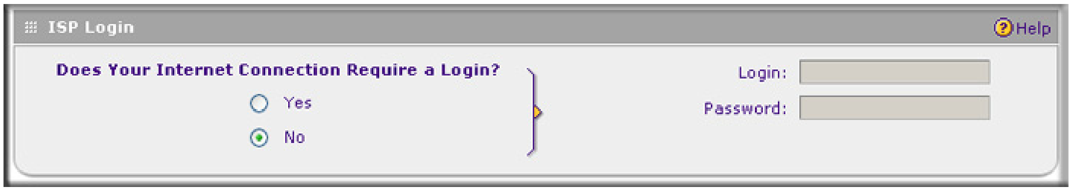
Each computer or router on your network has a unique 48-bit local Ethernet address. This is also referred to as the computer's Media Access Control (MAC) address. The default is set to **Use Default Address** on the WAN Advanced Options screens. If your ISP requires MAC authentication and another MAC address has been previously registered with your ISP, then you need to enter that address on the WAN Advanced Options screen for the corresponding WAN interface (see *Configure Advanced WAN Options* on page 51).

Manually Configure the Internet Connection

Unless your ISP automatically assigns your configuration via DHCP, you need to obtain configuration parameters from your ISP in order to manually establish an Internet connection. The settings for various connection types are listed in the previous table.

➤ **To manually configure the WAN ISP settings:**

1. Select **Network Configuration > WAN Settings**. The WAN screen displays (see *Figure 10* on page 25).
2. Click the **Edit** table button in the Action column of the WAN interface for which you want to automatically configure the connection to the Internet. The WAN ISP Settings screen displays (see *Figure 11* on page 26, which shows the WAN1 ISP Settings screen as an example).
3. Locate the IPS Login section on the screen:



Does Your Internet Connection Require a Login?

○ Yes

● No

Login:

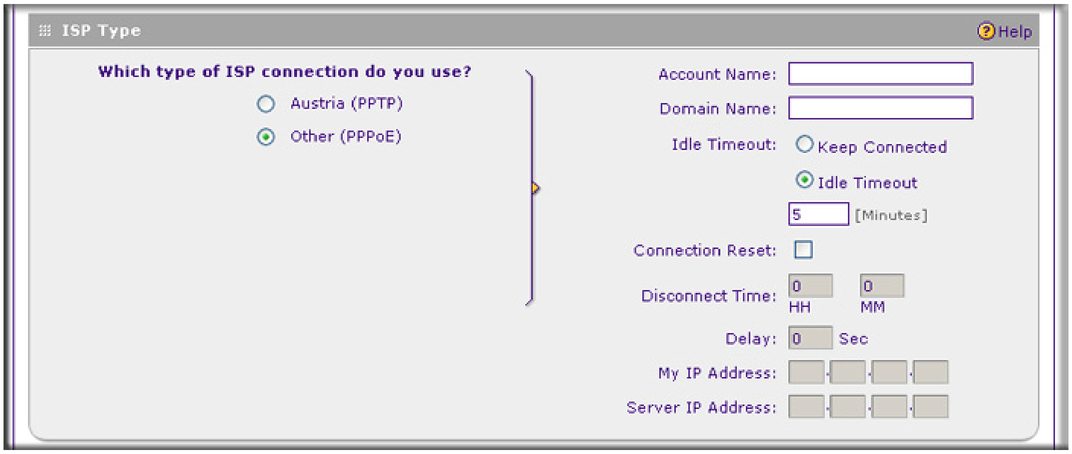
Password:

Figure 13.

In the ISP Login section, select one of the following options:

- If your ISP requires an initial login to establish an Internet connection, select **Yes**. (The default is **No**.)
- If a login is not required, select **No** and ignore the Login and Password fields.

4. If you selected **Yes**, enter the login name in the Login field and the password in the Password field. This information is provided by your ISP.
5. In the ISP Type section of the screen, select the type of ISP connection that you use from the three listed options. By default, **Other (PPPoE)** is selected, as shown in the following figure:



Which type of ISP connection do you use?

○ Austria (PPTP)

● Other (PPPoE)

Account Name:

Domain Name:

Idle Timeout: ○ Keep Connected ● Idle Timeout 5 [Minutes]

Connection Reset: □

Disconnect Time: 0 HH 0 MM

Delay: 0 Sec

My IP Address:

Server IP Address:

Figure 14.

6. If your connection is PPTP or PPPoE, your ISP requires an initial login. Enter the settings as explained in the following table:

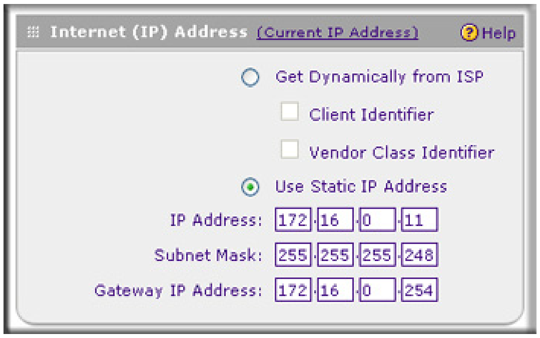
Table 3. PPTP and PPPoE settings

Setting	Description	
Austria (PPTP)	If your ISP is Austria Telecom or any other ISP that uses PPTP for login, select this radio button and enter the following settings:	
	Account Name	The account name is also known as the host name or system name. Enter the valid account name for the PPTP connection (usually your email ID assigned by your ISP). Some ISPs require you to enter your full email address here.
	Domain Name	Your domain name or workgroup name assigned by your ISP, or your ISP's domain name. You can leave this field blank.
	Idle Timeout	Select the **Keep Connected** radio button to keep the connection always on. To log out after the connection is idle for a period of time, select the **Idle Time** radio button and, in the timeout field, enter the number of minutes to wait before disconnecting. This is useful if your ISP charges you based on the period that you have logged in.
	My IP Address	The IP address assigned by the ISP to make the connection with the ISP server.

Table 3. PPTP and PPPoE settings (continued)

Setting	Description		
Austria (PPTP) (continued)	Server IP Address	The IP address of the PPTP server.	
Other (PPPoE)	If you have installed login software, then your connection type is PPPoE. Select this radio button and enter the following settings:		
	Account Name	The valid account name for the PPPoE connection.	
	Domain Name	The name of your ISP's domain or your domain name if your ISP has assigned one. You can leave this field blank.	
	Idle Timeout	Select the **Keep Connected** radio button to keep the connection always on. To log out after the connection is idle for a period of time, select the **Idle Time** radio button and, in the timeout field, enter the number of minutes to wait before disconnecting. This is useful if your ISP charges you based on the period that you have logged in.	
	Connection Reset	Select the **Connection Reset** check box to specify a time when the PPPoE WAN connection is reset, that is, the connection is disconnected momentarily and then reestablished. Then enter the following settings:	
		Disconnect Time	Specify the hour and minutes when the connection should be disconnected.
		Delay	Specify the period in seconds after which the connection should be reestablished.

7. In the Internet (IP) Address section of the screen, configure the IP address settings as explained in the following table. Click the **Current IP Address** link to see the currently assigned IP address.



○ Get Dynamically from ISP

□ Client Identifier

□ Vendor Class Identifier

● Use Static IP Address

IP Address: 172 . 16 . 0 . 11

Subnet Mask: 255 . 255 . 255 . 248

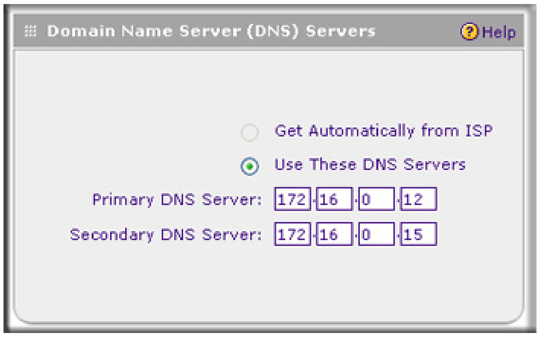
Gateway IP Address: 172 . 16 . 0 . 254

Figure 15.

Table 4. Internet IP address settings

Setting	Description	
Get Dynamically from ISP	If your ISP has not assigned you a static IP address, select the **Get Dynamically from ISP** radio button. The ISP automatically assigns an IP address to the VPN firewall using DHCP network protocol.	
	Client Identifier	Select the **Client Identifier** check box if your ISP requires the Client Identifier information to assign an IP address using DHCP.
	Vendor Class Identifier	Select the **Vendor Class Identifier** check box if your ISP requires the Vendor Class Identifier information to assign an IP address using DHCP.
Use Static IP Address	If your ISP has assigned you a fixed (static or permanent) IP address, select the **Use Static IP Address** radio button and enter the following settings:	
	IP Address	Static IP address assigned to you. This address identifies the VPN firewall to your ISP.
	Subnet Mask	The subnet mask is usually provided by your ISP.
	Gateway IP Address	The IP address of the ISP’s gateway is usually provided by your ISP.

8. In the Domain Name Server (DNS) Servers section of the screen, specify the DNS settings as explained in the following table.



○ Get Automatically from ISP

● Use These DNS Servers

Primary DNS Server: 172 . 16 . 0 . 12

Secondary DNS Server: 172 . 16 . 0 . 15

Figure 16.

Table 5. DNS server settings

Setting	Description	
Get Automatically from ISP	If your ISP has not assigned any Domain Name Server (DNS) addresses, select the **Get Automatically from ISP** radio button.	
Use These DNS Servers	If your ISP has assigned DNS addresses, select the **Use These DNS Servers** radio button. Ensure that you fill in valid DNS server IP addresses in the fields. Incorrect DNS entries might cause connectivity issues.	
	Primary DNS Server	The IP address of the primary DNS server.
	Secondary DNS Server	The IP address of the secondary DNS server.

9. Click **Test** to evaluate your entries. The VPN firewall attempts to make a connection according to the settings that you entered.
10. Click **Apply** to save any changes to the WAN ISP settings. (Or click **Reset** to discard any changes and revert to the previous settings.)

If you want to manually configure an additional WAN interface, select another WAN interface and repeat these steps. You can configure up to four WAN interfaces.

When you are finished, click the **Logout** link at the upper right corner of the web management interface or proceed to additional setup and management tasks.

Configure the WAN Mode

The VPN firewall can be configured on a mutually exclusive basis for either auto-rollover (for increased system reliability) or load balancing (for maximum bandwidth efficiency). If you do not select load balancing, you need to specify one WAN interface as the primary interface.

- **Load balancing mode**. The VPN firewall distributes the outbound traffic equally among the WAN interfaces that are functional. You can configure up to four WAN interfaces. The VPN firewall supports weighted load balancing and round-robin load balancing (see *Configure Load Balancing and Optional Protocol Binding* on page 36).

> **Note:** Scenarios could arise when load balancing needs to be bypassed for certain traffic or applications. If certain traffic needs to travel on a specific WAN interface, configure protocol binding rules for that WAN interface. The rule should match the desired traffic.

- **Primary WAN mode**. The selected WAN interface is made the primary interface. The other three interfaces are disabled.
- **Auto-rollover mode**. The selected WAN interface is defined as the primary link, and another interface needs to be defined as the rollover link. The remaining two interfaces are disabled. As long as the primary link is up, all traffic is sent over the primary link. When the primary link goes down, the rollover link is brought up to send the traffic. When the primary link comes back up, traffic automatically rolls back to the original primary link.

  If you want to use a redundant ISP link for backup purposes, select the WAN port that should function as the primary link for this mode. Ensure that the backup WAN port has also been configured and that you configure the WAN failure detection method on the WAN Advanced Options screen to support auto-rollover (see *Configure the Auto-Rollover Mode and Failure Detection Method* on page 34).

Whichever WAN mode you select, you need to also select either NAT or classical routing, as explained in the following sections.

Configure Network Address Translation

Network Address Translation (NAT) allows all PCs on your LAN to share a single public Internet IP address. From the Internet, there is only a single device (the VPN firewall) and a single IP address. PCs on your LAN can use any private IP address range, and these IP addresses are not visible from the Internet.

Note the following about NAT:

- The VPN firewall uses NAT to select the correct PC (on your LAN) to receive any incoming data.
- If you have only a single public Internet IP address, you need to use NAT (the default setting).
- If your ISP has provided you with multiple public IP addresses, you can use one address as the primary shared address for Internet access by your PCs, and you can map incoming traffic on the other public IP addresses to specific PCs on your LAN. This one-to-one inbound mapping is configured using an inbound firewall rule.

➢ **To configure NAT:**

1. Select **Network Configuration > WAN Settings > WAN Mode**. The WAN Mode screen displays (see *Figure 17* on page 34).
2. In the NAT (Network Address Translation) section of the screen select the **NAT** radio button.
3. Click **Apply** to save your settings.

Configure Classical Routing

In classical routing mode, the VPN firewall performs routing, but without NAT. To gain Internet access, each PC on your LAN needs to have a valid static Internet IP address.

If your ISP has allocated a number of static IP addresses to you, and you have assigned one of these addresses to each PC, you can choose classical routing. Or, you can use classical routing for routing private IP addresses within a campus environment.

To learn the status of the WAN ports, you can view the Router Status screen (see *View the System (Router) Status and Statistics* on page 275).

➢ **To configure classical routing:**

1. Select **Network Configuration > WAN Settings > WAN Mode**. The WAN Mode screen displays (see *Figure 17* on page 34).
2. In the NAT (Network Address Translation) section of the screen select the **Classical Routing** radio button.
3. Click **Apply** to save your settings.

Configure the Auto-Rollover Mode and Failure Detection Method

To use a redundant ISP link for backup purposes, ensure that the backup WAN interface has already been configured. Then select the WAN interface that will act as the primary link for this mode and configure the WAN failure detection method on the WAN Mode screen to support auto-rollover.

When the VPN firewall is configured in auto-rollover mode, it uses the selected WAN failure detection method to detect the status of the primary link connection at regular intervals. Link failure is detected in one of the following ways:

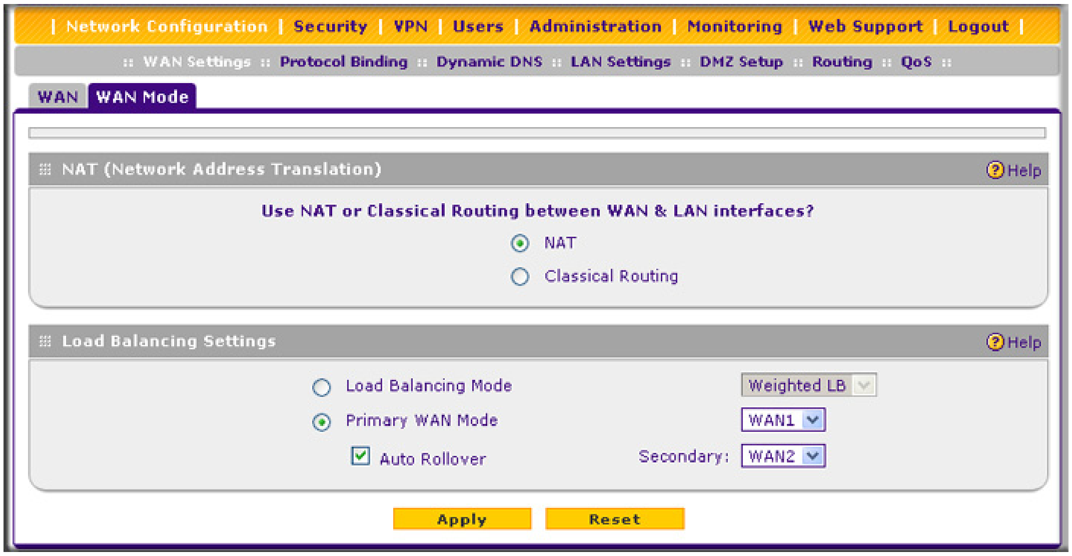
- By sending DNS queries to a DNS server
- By sending a ping request to an IP address
- None (no failure detection is performed)

From the primary WAN interface, DNS queries or ping requests are sent to the specified IP address. If replies are not received, after a specified number of retries, the primary WAN interface is considered down and a rollover to the backup WAN interface occurs. When the the primary WAN interface comes back up, another rollover occurs from the backup WAN interface back to the primary WAN interface. The WAN failure detection method that you select applies only to the primary WAN interface, that is, it monitors the primary link only.

Configure Auto-Rollover Mode

➢ **To configure auto-rollover mode:**

1. Select **Network Configuration > WAN Settings > WAN Mode**. The WAN Mode screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
WAN
WAN Mode
Help
Help
Apply
Reset

NAT (Network Address Translation)

Use NAT or Classical Routing between WAN & LAN interfaces?

● NAT

○ Classical Routing

Load Balancing Settings

○ Load Balancing Mode Weighted LB

● Primary WAN Mode WAN1

☑ Auto Rollover Secondary: WAN2

Figure 17.

2. In the Load Balancing Settings section of the screen, configure the following settings:
   - **a.** Select the **Primary WAN Mode** radio button.
   - **b.** From the corresponding drop-down list on the right, select a WAN interface to function as the primary WAN interface. The other WAN interfaces become disabled.
   - **c.** Select the **Auto Rollover** check box.
   - **d.** From the corresponding drop-down list on the right, select a WAN interface to function as the backup WAN interface.

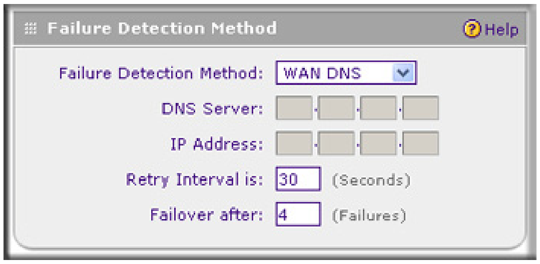
Note: Ensure that the backup WAN interface is configured before enabling auto-rollover mode.

3. Click **Apply** to save your settings.

Configure the Failure Detection Method

➢ **To configure failure detection method:**

1. Select **Network Configuration > WAN Settings**. The WAN screen displays (see *Figure 10* on page 25).
2. Click the **Edit** table button in the Action column of the WAN interface that you selected as the primary WAN interface. The WAN ISP Settings screen displays (see *Figure 11* on page 26, which shows the WAN1 ISP Settings screen as an example).
3. Click the **Advanced** option arrow in the upper right of the screen. The WAN Advanced Options screen displays for the WAN interface that you selected. (For an image of the entire screen, see *Figure 28* on page 52).
4. Locate the Failure Detection Method section on the screen. Enter the settings as explained in the following table.



Failure Detection Method: WAN DNS

DNS Server: . . .

IP Address: . . .

Retry Interval is: 30 (Seconds)

Failover after: 4 (Failures)

Figure 18.

Table 6. Failure detection method settings

Setting	Description
Failure Detection Method	Select a failure detection method from the drop-down list: • **WAN DNS**. DNS queries are sent to the DNS server that is configured in the Domain Name Server (DNS) Servers section of the WAN ISP screen (see *Manually Configure the Internet Connection* on page 28). • **Custom DNS**. DNS queries are sent to a DNS server that you need to specify in the DNS Server fields. • **Ping**. Pings are sent to a server with a public IP address that you need to specify in the IP Address fields. The server should not reject the ping request and should not consider ping traffic to be abusive. **Note:** DNS queries or pings are sent through the WAN interface that is being monitored. The retry interval and number of failover attempts determine how quickly the VPN firewall switches from the primary link to the backup link in case the primary link fails, or when the primary link comes back up, switches back from the backup link to the primary link.
DNS Server	The IP address of the DNS server.
IP Address	The IP address of the ping server.
Retry Interval is	The retry interval in seconds. The DNS query or ping is sent periodically after every test period. The default test period is 30 seconds.
Failover after	The number of failover attempts. The primary WAN interface is considered down after the specified number of queries have failed to elicit a reply. The backup interface is brought up after this situation has occurred. The failover default is 4 failures.

Note: The default time to roll over after the primary WAN interface fails is 2 minutes. The minimum test period is 30 seconds, and the minimum number of tests is 4.

5. Click **Apply** to save your settings.

You can configure the VPN firewall to generate a WAN status log and email this log to a specified address (see *Activate Notification of Events, Alerts, and Syslogs* on page 269).

Configure Load Balancing and Optional Protocol Binding

To use multiple ISP links simultaneously, configure load balancing. In load balancing mode, any WAN port carries any outbound protocol unless protocol binding is configured.

When a protocol is bound to a particular WAN port, all outgoing traffic of that protocol is directed to the bound WAN port. For example, if the HTTPS protocol is bound to the WAN1 port and the FTP protocol is bound to the WAN2 port, then the VPN firewall automatically routes all outbound HTTPS traffic from the computers on the LAN through the WAN1 port. All outbound FTP traffic is routed through the WAN2 port.

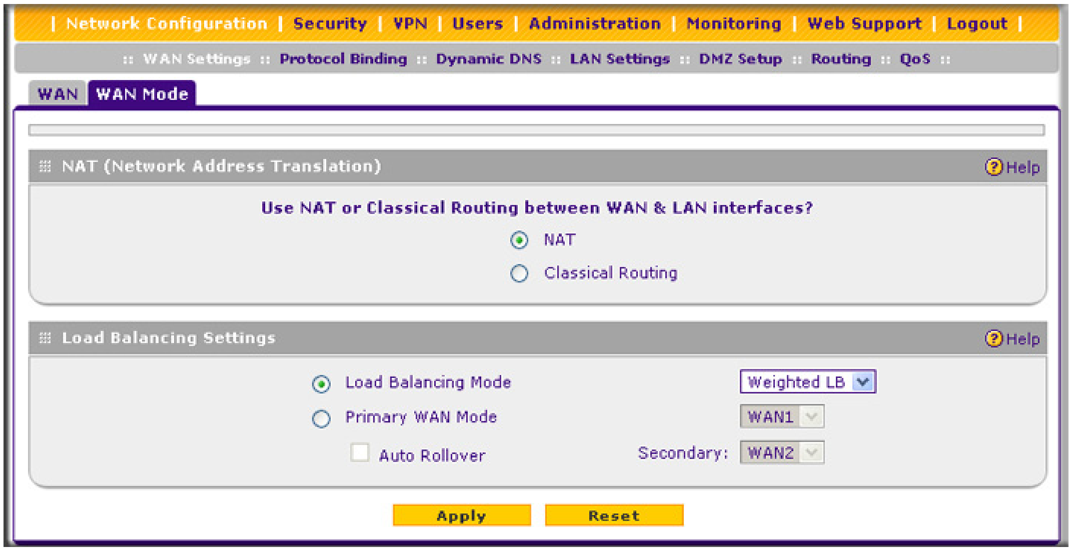
Protocol binding addresses two issues:

- Segregation of traffic between links that are not of the same speed.
  High-volume traffic can be routed through the WAN port connected to a high-speed link, and low-volume traffic can be routed through the WAN port connected to the low-speed link.
- Continuity of source IP address for secure connections.
  Some services, particularly HTTPS, cease to respond when a client's source IP address changes shortly after a session has been established.

Configure Load Balancing

➤ **To configure load balancing:**

1. Select **Network Configuration > WAN Settings > WAN Mode**. The WAN Mode screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
WAN
WAN Mode
Help
Help
Apply
Reset

NAT (Network Address Translation)

Use NAT or Classical Routing between WAN & LAN interfaces?

● NAT
○ Classical Routing

Load Balancing Settings

● Load Balancing Mode	Weighted LB
○ Primary WAN Mode	WAN1
□ Auto Rollover	Secondary: WAN2

Figure 19.

2. In the Load Balancing Settings section of the screen, configure the following settings:
   a. Select the **Load Balancing Mode** radio button.
   b. From the corresponding drop-down list on the right, select one of the following load balancing methods:
      - **Weighted LB**. With weighted load balancing, balance weights are calculated based on WAN link speed and available WAN bandwidth. This is the default setting and most efficient load-balancing algorithm.
      - **Round-robin**. With round-robin load balancing, new traffic connections are sent over a WAN link in a serial method irrespective of bandwidth or link speed. For example, if the WAN1, WAN2, and WAN3 interfaces are active in round-robin load balancing mode, an HTTP request could first be sent over the WAN1 interface,

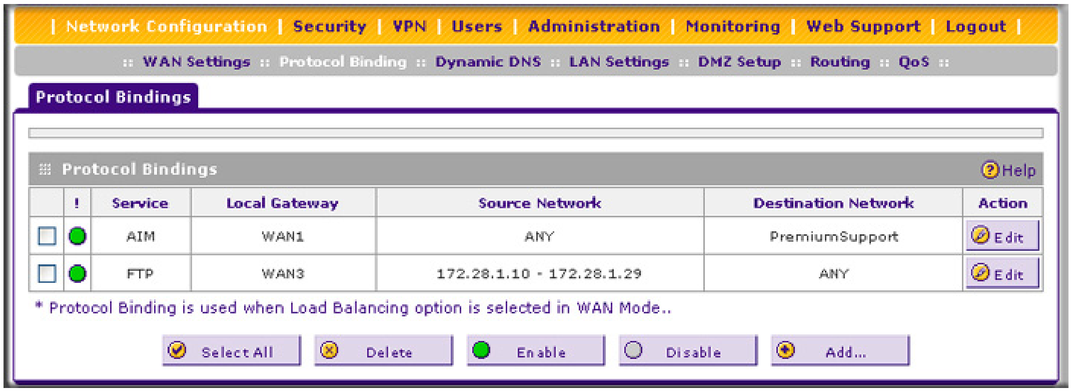
then a new FTP session could start on the WAN2 interface, and then any new connection to the Internet could be made on the WAN3 interface. This load-balancing method ensures that a single WAN interface does not carry a disproportionate distribution of sessions.

3. Click **Apply** to save your settings.

Configure Protocol Binding (Optional)

➤ **To configure protocol binding and add protocol binding rules:**

1. Select **Network Configuration > Protocol Binding**.
2. Select the **Load Balancing** radio button. The Protocol Bindings screen displays. (The following figure shows two examples in the Protocol Binding table.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
Protocol Bindings
Protocol Bindings
Help
Select All
Delete
Enable
Disable
Add...

	!	Service	Local Gateway	Source Network	Destination Network	Action
□	●	AIM	WAN1	ANY	PremiumSupport	Edit
□	●	FTP	WAN3	172.28.1.10 - 172.28.1.29	ANY	Edit

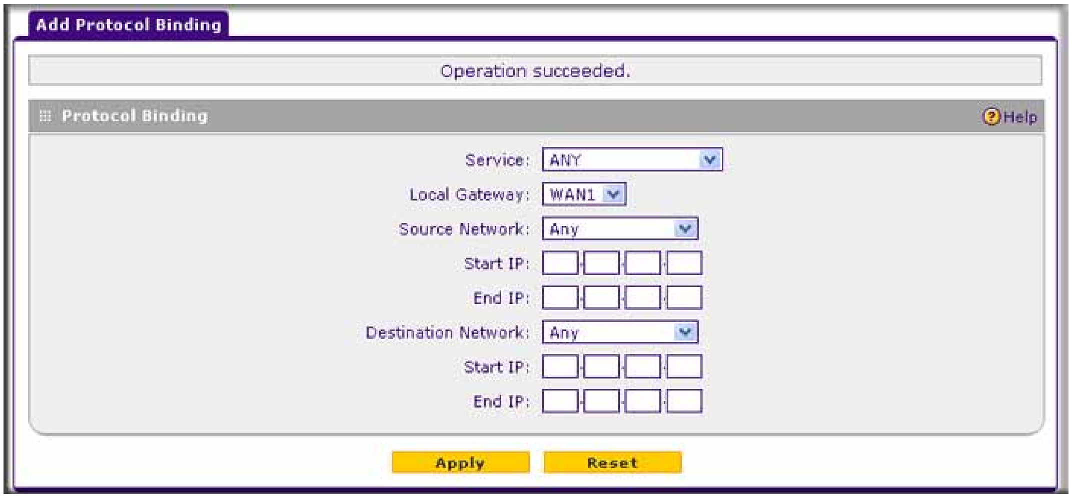
* Protocol Binding is used when Load Balancing option is selected in WAN Mode..

Figure 20.

The Protocol Binding table displays the following fields:

- **Check box**. Allows you to select the protocol binding rule in the table.
- **Status icon**. Indicates the status of the protocol binding rule:
  - Green circle. The protocol binding rule is enabled.
  - Gray circle. The protocol binding rule is disabled.
- **Service**. The service or protocol for which the protocol binding rule is set up.
- **Local Gateway**. The WAN interface to which the service or protocol is bound.
- **Source Network**. The computers or groups on your network that are affected by the protocol binding rule.
- **Destination Network**. The Internet locations (based on their IP address) or groups that are covered by the protocol binding rule.
- **Action**. The Edit table button provides access to the Edit Protocol Binding screen for the corresponding service.

3. Click the **Add** table button below the Protocol Binding table. The Add Protocol Binding screen displays:



Add Protocol Binding

Operation succeeded.

Protocol Binding

Service: ANY

Local Gateway: WAN1

Source Network: Any

Start IP:

End IP:

Destination Network: Any

Start IP:

End IP:

Figure 21.

4. Configure the protocol binding settings as explained in the following table:

Table 7. Add Protocol Binding screen settings

Setting	Description	
Service	From the drop-down list, select a service or application to be covered by this rule. If the service or application does not appear in the list, you need to define it using the Services screen (see *Services-Based Rules* on page 83).	
Local Gateway	From the drop-down list, select one of the WAN interfaces.	
Source Network	The source network settings determine which computers on your network are affected by this rule. Select one of the following options from the drop-down list:	
	Any	All devices on your LAN.
	Single address	In the Start IP field, enter the IP address to which the rule is applied.
	Address Range	In the Start IP field and End IP field, enter the IP addresses for the range to which the rule is applied.
	Group	If this option is selected, the rule is applied to the selected group. The group can be a LAN group or an IP (LAN) group. **Note:** For information about LAN group, see *Manage Groups and Hosts (LAN Groups)* on page 67. For information about IP groups, see *Create IP Groups* on page 114.).

Table 7. Add Protocol Binding screen settings (continued)

Setting	Description	
Destination Network	The destination network settings determine which Internet locations (based on their IP address) are covered by the rule. Select one of the following options from the drop-down list:	
	Any	All Internet IP address.
	Single address	In the Start IP field, enter the IP address to which the rule is applied.
	Address range	In the Start IP field and End IP field, enter the IP addresses for the range to which the rule is applied.
	Group	If this option is selected, the rule is applied to the selected IP (WAN) group. **Note:** For information about IP groups, see *Create IP Groups* on page 114.).

5. Click **Apply** to save your settings. The protocol binding rule is added to the Protocol Binding table. The rule is automatically enabled, which is indicated by the "!" status icon that displays a green circle.

➢ To edit a protocol binding:

1. On the Protocol Bindings screen (see *Figure 20* on page 38), in the Protocol Bindings table, click the **Edit** table button to the right of the binding that you want to edit. The Edit Protocol Bindings screen displays. This screen shows the same fields as the Add Protocol Bindings screen (see the previous figure).
2. Modify the settings as explained in the previous table.
3. Click **Apply** to save your settings.

➢ To enable, disable, or delete one or more protocol bindings:

1. On the Protocol Bindings screen (see *Figure 20* on page 38), select the check box to the left of the protocol binding that you want to enable, disable, or delete, or click the **Select All** table button to select all bindings.
2. Click one of the following table buttons:
   - **Enable**. Enables the binding or bindings. The "!" status icon changes from a gray circle to a green circle, indicating that the selected binding or bindings are enabled. (By default, when a binding is added to the table, it is automatically enabled.)
   - **Disable**. Disables the binding or bindings. The "!" status icon changes from a green circle to a gray circle, indicating that the selected binding or bindings are disabled.
   - **Delete**. Deletes the binding or bindings.

Configure Secondary WAN Addresses

You can set up a single WAN Ethernet port to be accessed through multiple IP addresses by adding aliases to the port. An alias is a secondary WAN address. One advantage is, for example, that you can assign different virtual IP addresses to a web server and an FTP server, even though both servers use the same physical IP address. You can add several secondary IP addresses to a single WAN port.

After you have configured secondary WAN addresses, these addresses are displayed on the following firewall rule screens:

- In the WAN Destination IP Address drop-down lists of the following inbound firewall rule screens:
  - Add LAN WAN Inbound Service screen
  - Add DMZ WAN Inbound Service screen
- In the NAT IP drop-down lists of the following outbound firewall rule screens:
  - Add LAN WAN Outbound Service screen
  - Add DMZ WAN Outbound Service screen

For more information about firewall rules, see *Use Rules to Block or Allow Specific Kinds of Traffic* on page 82).

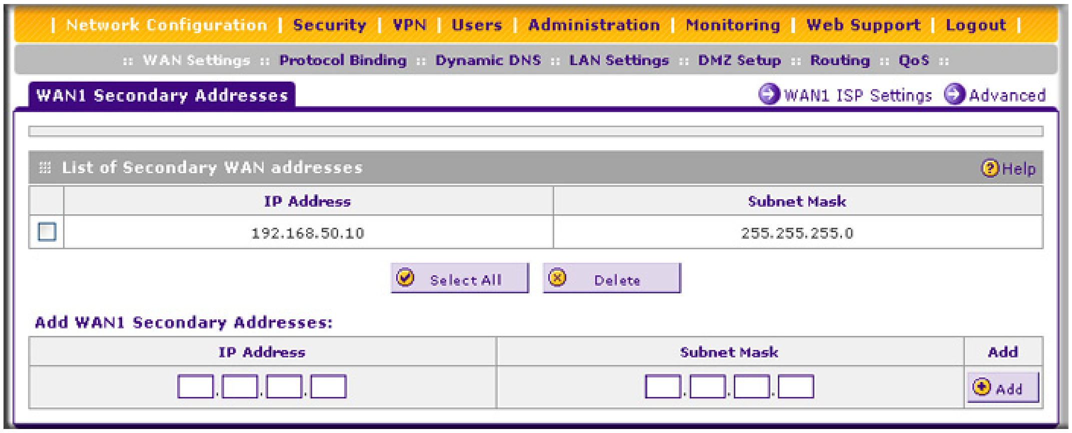
Note: It is important that you ensure that any secondary WAN addresses are different from the primary WAN, LAN, and DMZ IP addresses that are already configured on the VPN firewall. However, primary and secondary WAN addresses can be in the same subnet. The following is an example of correctly configured IP addresses:

Primary WAN1 IP address: 10.0.0.1 with subnet 255.0.0.0
Secondary WAN1 IP: 30.0.0.1 with subnet 255.0.0.0
Primary WAN2 IP address: 20.0.0.1 with subnet 255.0.0.0
Secondary WAN2 IP: 40.0.0.1 with subnet 255.0.0.0
DMZ IP address: 192.168.10.1 with subnet 255.255.255.0
Primary LAN IP address: 192.168.1.1 with subnet 255.255.255.0
Secondary LAN IP: 192.168.20.1 with subnet 255.255.255.0

➢ **To add a secondary WAN address to a WAN port:**

1. Select **Network Configuration > WAN Settings**. The WAN screen displays (see *Figure 10* on page 25).
2. Click the **Edit** table button in the Action column of the WAN interface for which you want to add a secondary address. The WAN ISP Settings screen displays (see *Figure 11* on page 26, which shows the WAN1 ISP Settings screen as an example).

3. Click the **Secondary Addresses** option arrow in the upper right of the screen. The WAN Secondary Addresses screen displays for the WAN interface that you selected. (The following figure see shows the WAN1 Secondary Addresses screen as an example and includes one entry in the List of Secondary WAN addresses table.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
WAN1 Secondary Addresses
WAN1 ISP Settings
Advanced
Help
Select All
Delete
Add

List of Secondary WAN addresses

	IP Address	Subnet Mask
□	192.168.50.10	255.255.255.0

Add WAN1 Secondary Addresses:

IP Address	Subnet Mask	Add
. . .	. . .	Add

Figure 22.

The List of Secondary WAN addresses table displays the secondary LAN IP addresses added for the selected WAN interface.

4. In the Add WAN Secondary Addresses section of the screen, enter the following settings:
   - **IP Address**. Enter the secondary address that you want to assign to the WAN port.
   - **Subnet Mask**. Enter the subnet mask for the secondary IP address.
5. Click the **Add** table button in the rightmost column to add the secondary IP address to the List of Secondary WAN addresses table.

   Repeat *step 4* and *step 5* for each secondary IP address that you want to add to the List of Secondary WAN addresses table.

➢ **To delete one ore more secondary addresses:**

1. In the List of Secondary WAN addresses table, select the check box to the left of the address that you want to delete, or click the **Select All** table button to select all addresses.
2. Click the **Delete** table button.

Configure Dynamic DNS

Dynamic DNS (DDNS) is an Internet service that allows devices with varying public IP addresses to be located using Internet domain names. To use DDNS, you need to set up an account with a DDNS provider such as DynDNS.org, TZO.com, Oray.net, or 3322.org. (Links to DynDNS, TZO, Oray, and 3322 are provided for your convenience as option arrows on the DDNS configuration screens.) The VPN firewall firmware includes software that notifies DDNS servers of changes in the WAN IP address, so that the services running on this network can be accessed by others on the Internet.

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will not know in advance what your IP address will be, and the address can change frequently—hence, the need for a commercial DDNS service, which allows you to register an extension to its domain, and restores DNS requests for the resulting FQDN to your frequently changing IP address.

After you have configured your account information on the VPN firewall, when your ISP-assigned IP address changes, your VPN firewall automatically contacts your DDNS service provider, logs in to your account, and registers your new IP address. Consider the following:

- For auto-rollover mode, you need a fully qualified domain name (FQDN) to implement features such as exposed hosts and virtual private networks regardless of whether you have a fixed or dynamic IP address.
- For load balancing mode, you might still need a fully qualified domain name (FQDN) either for convenience or if you have a dynamic IP address.

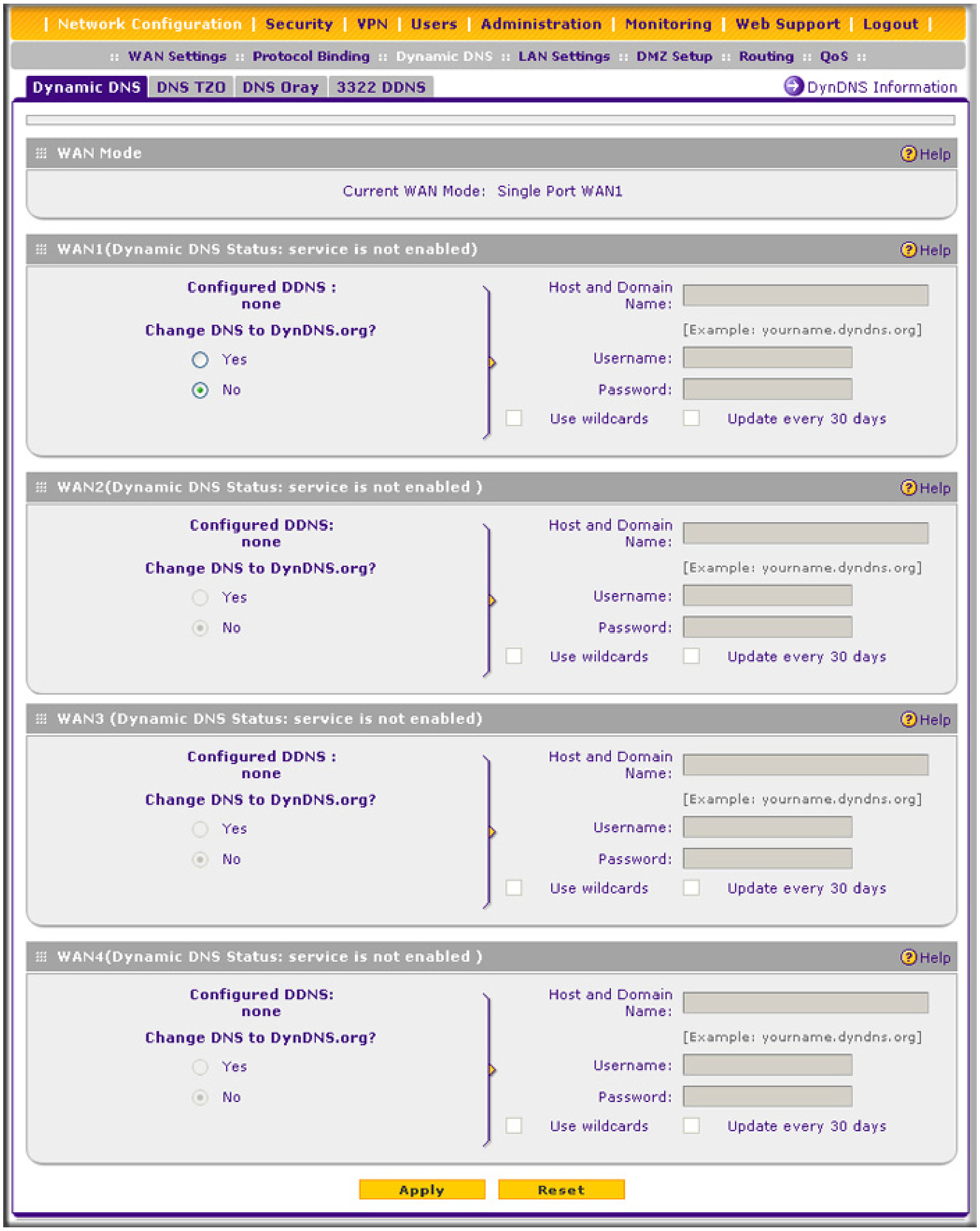
Note: If your ISP assigns a private WAN IP address such as 192.168.x.x or 10.x.x.x, the DDNS service does not work because private addresses are not routed on the Internet.

➢ **To configure DDNS:**

1. Select **Network Configuration > Dynamic DNS**. The Dynamic DNS screen displays (see the following figure).

   The WAN Mode section on the screen reports the currently configured WAN mode (for example, Single Port WAN1, Load Balancing, or Auto Rollover). Only those options that match the configured WAN mode are accessible on the screen.

2. Select the submenu tab for your DDNS service provider:
   - **Dynamic DNS** (which is shown in the following figure) for DynDNS.org
   - **DNS TZO** for TZO.com
   - **DNS Oray** for Oray.net
   - **3322 DDNS** for 3322.org


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
Dynamic DNS
DNS TZO
DNS Oray
3322 DDNS
DynDNS Information
Help
Apply
Reset

WAN Mode

Current WAN Mode: Single Port WAN1

WAN1(Dynamic DNS Status: service is not enabled)

Configured DDNS : none

Change DNS to DynDNS.org?

○ Yes
● No

Host and Domain Name:

[Example: yourname.dyndns.org]

Username:

Password:

□ Use wildcards □ Update every 30 days

WAN2(Dynamic DNS Status: service is not enabled)

Configured DDNS: none

Change DNS to DynDNS.org?

○ Yes
● No

Host and Domain Name:

[Example: yourname.dyndns.org]

Username:

Password:

□ Use wildcards □ Update every 30 days

WAN3 (Dynamic DNS Status: service is not enabled)

Configured DDNS : none

Change DNS to DynDNS.org?

○ Yes
● No

Host and Domain Name:

[Example: yourname.dyndns.org]

Username:

Password:

□ Use wildcards □ Update every 30 days

WAN4(Dynamic DNS Status: service is not enabled)

Configured DDNS: none

Change DNS to DynDNS.org?

○ Yes
● No

Host and Domain Name:

[Example: yourname.dyndns.org]

Username:

Password:

□ Use wildcards □ Update every 30 days

Figure 23.

3. Click the **Information** option arrow in the upper right of a DNS screen for registration information.

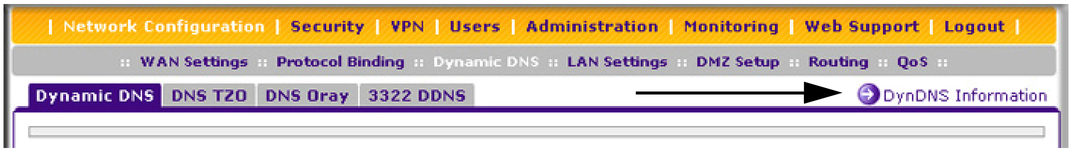

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
Dynamic DNS
DNS TZO
DNS Oray
3322 DDNS
DynDNS Information

Figure 24.

4. Access the website of the DDNS service provider and register for an account (for example, for DynDNS.org, go to *http://www.dyndns.com/*).
5. Configure the DDNS service settings as explained in the following table:

Table 8. DDNS service settings

Setting	Description	
WAN1 (Dynamic DNS Status: ...)		
Change DNS to (DynDNS, TZO, Oray, or 3322)	Select the **Yes** radio button to enable the DDNS service. The fields that display on the screen depend on the DDNS service provider that you have selected. Enter the following settings:	
	Host and Domain Name	The host and domain name for the DDNS service.
	Username or User Email Address	The user name or email address for DDNS server authentication.
	Password or User Key	The password that is used for DDNS server authentication.
	Use wildcards	If your DDNS provider allows the use of wildcards in resolving your URL, you can select the **Use wildcards** check box to activate this feature. For example, the wildcard feature causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org.
	Update every 30 days	If your WAN IP address does not change often, you might need to force a periodic update to the DDNS service to prevent your account from expiring. If it appears, you can select the **Update every 30 days** check box to enable a periodic update.
WAN2 (Dynamic DNS Status: ...) **WAN3 (Dynamic DNS Status: ...)** **WAN4 (Dynamic DNS Status: ...)**		
See the information for WAN1 above about how to enter the settings. You can select different DDNS services for different WAN interfaces.		

6. Click **Apply** to save your configuration.

Configure WAN QoS Profiles

The VPN firewall can support multiple quality of service (QoS) profiles for each WAN interface. You can assign profiles to services such as HTTP, FTP, and DNS and to LAN groups or IP addresses. Profiles enforce either rate control with bandwidth allocation or priority queue control. You can configure both types of profiles, but either all profiles on the VPN firewall enforce rate control and the profiles that you configured for priority queue control are inactive, or the other way around. Both types of profiles cannot be active simultaneously.

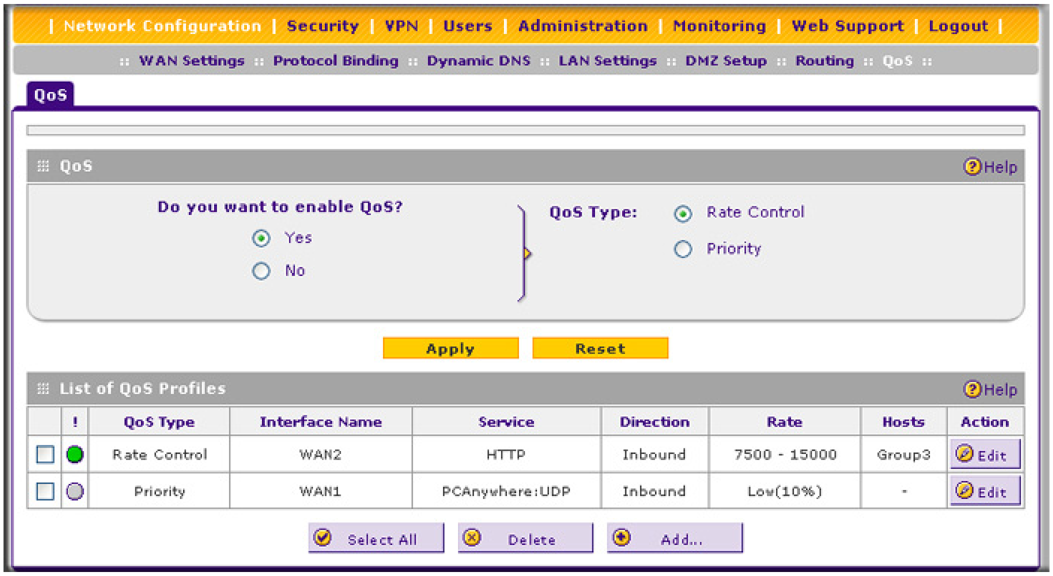
- **Rate control with bandwidth allocation**. These types of profiles specify how bandwidth is distributed among the services and hosts. A profile with a high priority is offered excess bandwidth while the required bandwidth is still allocated to profiles that specify minimum and maximum bandwidth rates. The congestion priority represents the classification level of the packets among the priority queues within the system. If you select a default congestion priority, traffic is mapped based on the Type of Service (ToS) field in the packet's IP header.
- **Priority queue control**. These types of profiles specify the priority levels of the services. You can select a high priority queue or a low priority queue. Services in the high priority queue share 60 percent of the interface bandwidth; services in the low priority queue share 10 percent of the interface bandwidth. By default, all services are assigned the medium priority queue in which they share 30 percent of the interface bandwidth.

Both types of profiles let you allocate the Differentiated Services (DiffServ) QoS packet matching and QoS packet marking settings, which you configure by specifying Differentiated Services Code Point (DSCP) values, from 0 to 63.

Note: Before you enable WAN QoS, make sure that the WAN connection type and speeds are configured correctly in the Upload/Download Settings section of the WAN Advanced screen for the WAN interface (see *Configure Advanced WAN Options* on page 51).

➢ **To enable and configure QoS for WAN interfaces:**

1. Select **Network Configuration > QoS**. The QoS screen displays. (The following screen shows some profiles in the List of QoS Profiles table).


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
QoS
Help
Apply
Reset
Select All
Delete
Add...

QoS

Do you want to enable QoS?

● Yes

○ No

QoS Type: ● Rate Control ○ Priority

List of QoS Profiles

	!	QoS Type	Interface Name	Service	Direction	Rate	Hosts	Action
□	🟢	Rate Control	WAN2	HTTP	Inbound	7500 - 15000	Group3	Edit
□	○	Priority	WAN1	PCAnywhere:UDP	Inbound	Low(10%)	-	Edit

Figure 25.

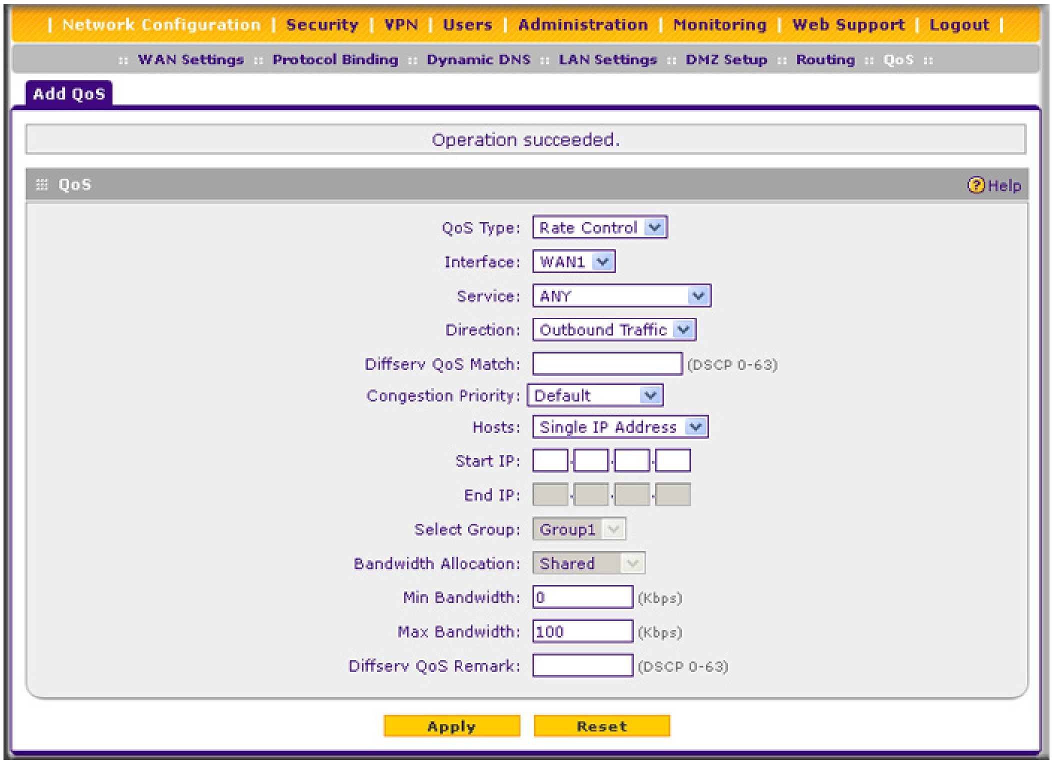
2. To enable QoS, select the **Yes** radio button. By default, the No radio button is selected.
3. Specify the profile type that should be active by selecting one of the following radio buttons.
   - **Rate control**. All rate control QoS profiles that you configure are active but priority QoS profiles are not.
   - **Priority**. All priority QoS profiles that you configure are active but priority rate control profiles are not.
4. Click **Apply** to save your settings.

   The List of QoS Profiles table shows the following columns, all of which are explained in detail in the following table and *Table 10* on page 50.

   - **QoS Type**. The type of profile, either Rate Control or Priority.
   - **Interface**. The WAN interface to which the profile applies (WAN1, WAN2, WAN3, or WAN4).
   - **Service**. The service to which the profile applies.
   - **Direction**. The WAN direction to which the profile applies (inbound, outbound, or both).
   - **Rate**. The bandwidth rate in Kbps or priority.
   - **Hosts**. The IP address, IP addresses, or group to which the rate control profile applies. (The information in this column is not applicable to priority profiles).
   - **Action**. The Edit table button provides access to the Edit QoS screen for the corresponding profile.

➢ To add a rate control QoS profile:

1. Select **Network Configuration > QoS**. The QoS screen displays.
2. Under the List of QoS Profiles table, click the **Add** table button. The Add QoS screen displays. The following figure shows settings for a rate control QoS profile:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
Add QoS
QoS
Help
Apply
Reset

Operation succeeded.

QoS Type: Rate Control

Interface: WAN1

Service: ANY

Direction: Outbound Traffic

Diffserv QoS Match: (DSCP 0-63)

Congestion Priority: Default

Hosts: Single IP Address

Start IP:

End IP:

Select Group: Group1

Bandwidth Allocation: Shared

Min Bandwidth: 0 (Kbps)

Max Bandwidth: 100 (Kbps)

Diffserv QoS Remark: (DSCP 0-63)

Figure 26.

3. Enter the settings as explained in the following table:

Table 9. Add QoS screen settings for a rate control profile

Setting	Description
QoS Type	Rate Control (for Priority, see *Figure 27* on page 50 and *Table 10* on page 50)
Interface	From the drop-down list, select one of the WAN interfaces.
Service	From the drop-down list, select a service or application to be covered by this profile. If the service or application does not appear in the list, you need to define it using the Services screen (see *Services-Based Rules* on page 83).
Direction	From the drop-down list, select the direction to which rate control is applied: • **Outbound Traffic**. Rate control is applied to outbound traffic only. • **Inbound Traffic**. Rate control is applied to inbound traffic only.
Diffserv QoS Match	Enter a DSCP value in the range of 0 through 63. Packets are classified against this value. Leave this field blank to disable packet matching.

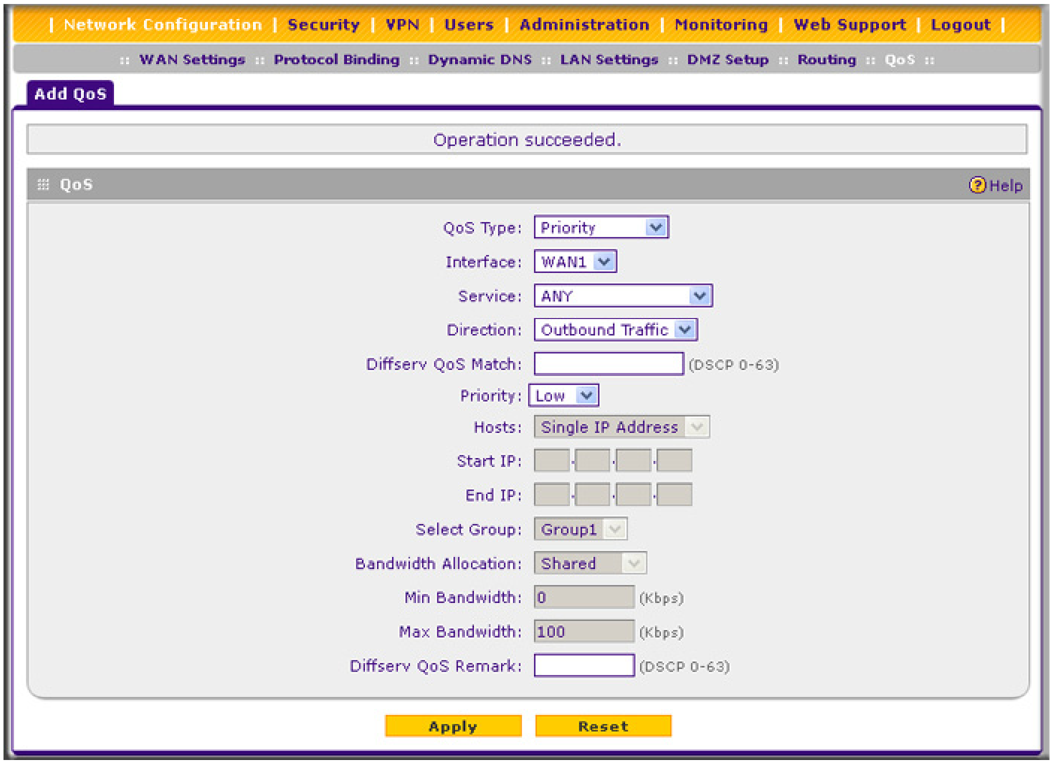
Table 9. Add QoS screen settings for a rate control profile (continued)

<table>
<tr><th>Setting</th><th colspan="2">Description</th></tr>
<tr><td>Congestion Priority</td><td colspan="2">From the drop-down list, select the priority queue that determines the allocation of excess bandwidth and the classification level of the packets among other priority queues on the VPN firewall:
• **Default**. Traffic is mapped based on the ToS field in the packet’s IP header.
• **High**. This queue includes the following DSCP values: AF41, AF42, AF43, AF44, and CS4.
• **Medium-high**. This queue includes the following DSCP values: AF31, AF32, AF33, AF34, and CS3.
• **Medium**. This queue includes the following DSCP values: AF21, AF22, AF23, AF24, and CS2.
• **Low**. This queue includes the following DSCP values: AF11, AF12, AF13, AF14, CS1, 0, and all other values.</td></tr>
<tr><td rowspan="5">Hosts</td><td colspan="2">From the drop-down list, select the IP address, range of IP addresses, or group to which the profile is applied:
• **Single IP Address**. The profile is applied to a single IP address. Enter the address in the Start IP field.
• **IP Address Range**. The profile is applied to an IP address range. Enter the start address of the range in the Start IP field and the end address of the range in the End IP field.
• **Group**. The profile is applied to a group. Select the group from the Select Group drop-down list and specify how the bandwidth is allocated by making a selection from the Bandwidth Allocation drop-down list.</td></tr>
<tr><td>Start IP</td><td>The IP address for a single IP address or the start IP address for an IP address range.</td></tr>
<tr><td>End IP</td><td>The end start IP address for an IP address range.</td></tr>
<tr><td>Select Group</td><td>From the drop-down list, select the LAN group to which the profile is applied. For information about LAN groups, see *Manage Groups and Hosts (LAN Groups)* on page 67.</td></tr>
<tr><td>Bandwidth Allocation</td><td>From the drop-down list and specify how the bandwidth is allocated:
• **Shared**. The bandwidth is shared among all members of the group.
• **Individual**. The bandwidth is allocated to each member of the group.</td></tr>
<tr><td>Min Bandwidth</td><td colspan="2">Enter the minimum bandwidth in Kbps that is allocated to the host. The default value is 0 Kbps.</td></tr>
<tr><td>Max Bandwidth</td><td colspan="2">Enter the maximum bandwidth in Kbps that is allocated to the host. The default value is 100 Kbps.</td></tr>
<tr><td>Diffserv QoS Remark</td><td colspan="2">Enter a DSCP value in the range of 0 through 63. Packets are marked with this value. Leave this field blank to disable packet marking.</td></tr>
</table>

4. Click **Apply** to save your settings. The profile is added to the List Of QoS Profiles table on the QoS screen.

➢ To add a priority QoS profile:

1. Select **Network Configuration > QoS**. The QoS screen displays.
2. Under the List of QoS Profiles table, click the **Add** table button. The Add QoS screen displays. The following figure shows settings for a priority QoS profile:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
Add QoS
Help
Apply
Reset

Operation succeeded.

QoS

QoS Type: Priority
Interface: WAN1
Service: ANY
Direction: Outbound Traffic
Diffserv QoS Match: (DSCP 0-63)
Priority: Low
Hosts: Single IP Address
Start IP: . . .
End IP: . . .
Select Group: Group1
Bandwidth Allocation: Shared
Min Bandwidth: 0 (Kbps)
Max Bandwidth: 100 (Kbps)
Diffserv QoS Remark: (DSCP 0-63)

Figure 27.

3. Enter the settings as explained in the following table:

Table 10. Add QoS screen settings for a priority profile

Setting	Description
QoS Type	Priority (for Rate Control, see *Figure 26* on page 48 and *Table 9* on page 48)
Interface	From the drop-down list, select one of the WAN interfaces.
Service	From the drop-down list, select a service or application to be covered by this profile. If the service or application does not appear in the list, you need to define it using the Services screen (see *Services-Based Rules* on page 83).
Direction	From the drop-down list, select the direction to which the priority queue is applied: • **Outbound Traffic**. The priority queue is applied to outbound traffic only. • **Inbound Traffic**. The priority queue is applied to inbound traffic only.
Diffserv QoS Match	Enter a DSCP value in the range of 0 through 63. Packets are classified against this value. Leave this field blank to disable packet matching.

Table 10. Add QoS screen settings for a priority profile (continued)

Setting	Description
Priority	From the drop-down list, select the priority queue that determines the allocation of bandwidth: • **Low**. All services that are assigned a low priority queue share 10 percent of interface bandwidth. • **High**. All services that are assigned a high priority queue share 60 percent of interface bandwidth. **Note:** By default, all services are assigned the medium priority queue in which they share 30 percent of the interface bandwidth.
Hosts	These settings are not applicable to a priority profile.
Start IP	
End IP	
Select Group	
Bandwidth Allocation	
Min Bandwidth	
Max Bandwidth	
Diffserv QoS Remark	Enter a DSCP value in the range of 0 through 63. Packets are marked with this value. Leave this field blank to disable packet marking.

4. Click **Apply** to save your settings. The profile is added to the List Of QoS Profiles table on the QoS screen.

➤ **To edit a QoS profile:**

1. In the Custom Services table, click the **Edit** table button to the right of the profile that you want to edit. The Edit QoS screen displays. This screen shows the same fields as the Add QoS screen (see the previous two figures).
2. Modify the settings as explained in the previous two tables.
3. Click **Apply** to save your settings.

➤ **To delete a QoS profile:**

1. In the Custom Services table, select the check box to the left of the QoS profile that you want to delete, or click the **Select All** table button to select all profiles.
2. Click the **Delete** table button.

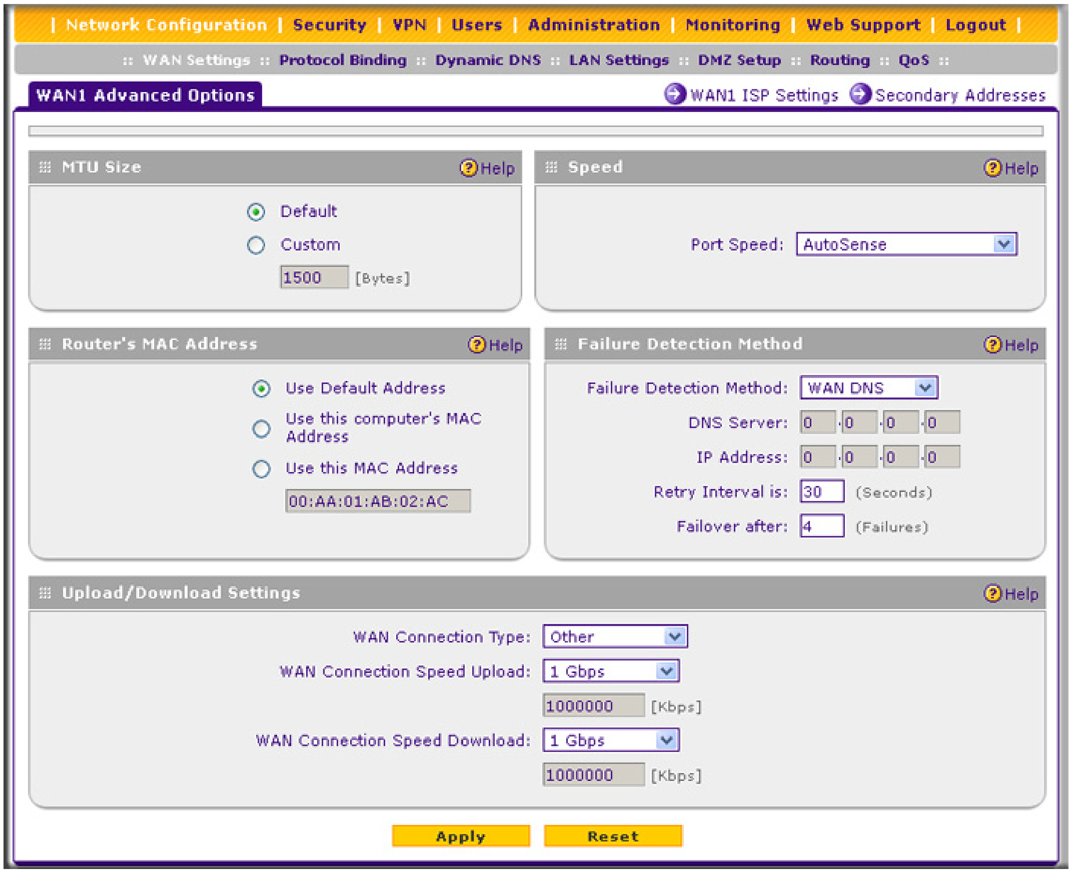
Configure Advanced WAN Options

The advanced options include configuration of the maximum transmission unit (MTU) size, port speed, VPN firewall’s MAC address, and setting a rate limit on the traffic that is being forwarded by the VPN firewall.

Note: You can also configure the failure detection method for the auto-rollover mode on the Advanced screen. This procedure is discussed in *Configure the Failure Detection Method* on page 35.

➤ **To configure advanced WAN options:**

1. Select **Network Configuration > WAN Settings**.
2. Click the **Edit** table button in the Action column of the WAN interface for which you want to configure the advanced options. The WAN ISP Settings screen displays (see *Figure 11* on page 26, which shows the WAN1 ISP Settings screen as an example).
3. Click the **Advanced** option arrow in the upper right of the screen. The WAN Advanced Options screen displays for the WAN interface that you selected. (The following figure shows the WAN1 Advanced Options screen as an example.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
WAN1 Advanced Options
WAN1 ISP Settings
Secondary Addresses
Help
Apply
Reset

MTU Size

● Default
○ Custom
1500 [Bytes]

Speed

Port Speed: AutoSense

Router's MAC Address

● Use Default Address
○ Use this computer's MAC Address
○ Use this MAC Address
00:AA:01:AB:02:AC

Failure Detection Method

Failure Detection Method: WAN DNS
DNS Server: 0 . 0 . 0 . 0
IP Address: 0 . 0 . 0 . 0
Retry Interval is: 30 (Seconds)
Failover after: 4 (Failures)

Upload/Download Settings

WAN Connection Type: Other
WAN Connection Speed Upload: 1 Gbps
1000000 [Kbps]
WAN Connection Speed Download: 1 Gbps
1000000 [Kbps]

Figure 28.

4. Enter the settings as explained in the following table:

Table 11. WAN Advanced Options screen settings

Setting	Description
MTU Size Make one of the following selections:	
Default	Select the **Default** radio button for the normal maximum transmit unit (MTU) value. For most Ethernet networks this value is 1500 Bytes, or 1492 Bytes for PPPoE connections.
Custom	Select the **Custom** radio button and enter an MTU value in the Bytes field. For some ISPs, you might need to reduce the MTU. This is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
Speed	
In most cases, the VPN firewall can automatically determine the connection speed of the WAN port of the device (modem or router) that provides the WAN connection. If you cannot establish an Internet connection, you might need to manually select the port speed. If you know the Ethernet port speed of the modem or router, select it from the drop-down list. Use the half-duplex settings only of the full-duplex settings do not function correctly. Select one of the following speeds from the drop-down list: • **AutoSense**. Speed autosensing. This is the default setting, which can sense 1000BaseT speed at full duplex. • **10BaseT Half_Duplex**. Ethernet speed at half duplex. • **10BaseT Full_Duplex**. Ethernet speed at full duplex. • **100BaseT Half_Duplex**. Fast Ethernet speed at half duplex. • **100BaseT Full_Duplex**. Fast Ethernet speed at full duplex. • **1000BaseT Full_Duplex**. Gigabit Ethernet.	
Router's MAC Address Make one of the following selections:	
Use Default Address	Each computer or router on your network has a unique 32-bit local Ethernet address. This is also referred to as the computer's Media Access Control (MAC) address. To use the VPN firewall's own MAC address, select the **Use Default Address** radio button.
Use this computer's MAC Address	Select the **Use this computer's MAC Address** radio button to allow the VPN firewall to use the MAC address of the computer you are now using to access the web management interface. This setting is useful if your ISP requires MAC authentication.
Use this MAC Address	Select the **Use this MAC Address** radio button to manually enter the MAC address in the field next to the radio button. You would typically enter the MAC address that your ISP is requiring for MAC authentication. **Note:** The format for the MAC address is 01:23:45:67:89:AB (numbers 0–9 and either uppercase or lowercase letters A–F). If you enter a MAC address, the existing entry is overwritten.
Failure Detection Method See *Configure the Failure Detection Method* on page 35, including *Table 6* on page 36.	

Table 11. WAN Advanced Options screen settings (continued)

Setting	Description
Upload/Download Settings These settings rate-limit the traffic that is being forwarded by the VPN firewall.	
WAN Connection Type	From the drop-down list, select the type of connection that the VPN firewall uses to connect to the Internet: **DSL**, **ADLS**, **Cable Modem**, **T1**, **T3**, or **Other**.
WAN Connection Speed Upload	From the drop-down list, select the maximum upload speed that is provided by your ISP. You can select from 56 Kbps to 1 Gbps, or you can select **Custom** and enter the speed in Kbps in the field below the drop-down list.
WAN Connection Speed Download	From the drop-down list, select the maximum download speed that is provided by your ISP. You can select from 56 Kbps to 1 Gbps, or you can select **Custom** and enter the speed in Kbps in the field below the drop-down list.

5. Click **Apply** to save your changes.

WARNING!

Depending on the changes that you made, when you click Apply, the VPN firewall might restart, or services such as HTTP and SMTP might restart.

If you want to configure the advanced settings for an additional WAN interface, select another WAN interface and repeat these steps.

Additional WAN-Related Configuration Tasks

- If you want the ability to manage the VPN firewall remotely, enable remote management (see *Configure Remote Management Access* on page 250). If you enable remote management, NETGEAR strongly recommend that you change your password (see *Change Passwords and Administrator Settings* on page 248).
- You can set up the traffic meter for each WAN, if desired. See *Enable the WAN Traffic Meter* on page 263.

What to Do Next

The following sections describe important tasks that you might want to address before you deploy the VPN firewall in your network:

- *Configure VPN Authentication Domains, Groups, and Users* on page 219
- *Manage Digital Certificates* on page 234
- *Use the IPSec VPN Wizard for Client and Gateway Configurations* on page 136
- *Overview of the SSL Configuration Process* on page 197

3. LAN Configuration 3

This chapter describes how to configure the advanced LAN features of your VPN firewall. This chapter contains the following sections:

Manage Virtual LANs and DHCP Options

A local area network (LAN) can generally be defined as a broadcast domain. Hubs, bridges, or switches in the same physical segment or segments connect all endpoints. Endpoints can communicate with each other without the need for a router. Routers connect LANs together, routing the traffic to the appropriate port.

A virtual LAN (VLAN) is a local area network with a definition that maps workstations on some basis other than geographic location (for example, by department, type of user, or primary application). To enable traffic to flow between VLANs, traffic needs to go through a router, just as if the VLANs were on two separate LANs.

A VLAN is a group of PCs, servers, and other network resources that behave as if they were connected to a single network segment—even though they might not be. For example, all marketing personnel might be spread throughout a building. Yet if they are all assigned to a single VLAN, they can share resources and bandwidth as if they were connected to the same segment. The resources of other departments can be invisible to the marketing VLAN members, accessible to all, or accessible only to specified individuals, depending on how the IT manager has set up the VLANs.

VLANs have a number of advantages:

- They make it easy to set up network segmentation. Users who communicate most frequently with each other can be grouped into common VLANs, regardless of physical location. Each group's traffic is contained largely within the VLAN, reducing extraneous traffic and improving the efficiency of the whole network.

- They are easy to manage. The addition of nodes, as well as moves and other changes, can be dealt with quickly and conveniently from a management interface rather than from the wiring closet.
- They provide increased performance. VLANs free up bandwidth by limiting node-to-node and broadcast traffic throughout the network.
- They ensure enhanced network security. VLANs create virtual boundaries that can be crossed only through a router. So standard, router-based security measures can be used to restrict access to each VLAN.

Port-Based VLANs

The VPN firewall supports port-based VLANs. Port-based VLANs help to confine broadcast traffic to the LAN ports. Even though a LAN port can be a member of more than one VLAN, the port can have only one VLAN ID as its port VLAN identifier (PVID). By default, all four LAN ports of the VPN firewall are assigned to the default VLAN, or VLAN 1. Therefore, by default, all four LAN ports have the default PVID 1. However, you can assign another PVID to a LAN port by selecting a VLAN profile from the drop-down list on the LAN Setup screen.

After you have created a VLAN profile and assigned one or more ports to the profile, you first need to enable the profile to activate it.

The VPN firewall's default VLAN cannot be deleted. All untagged traffic is routed through the default VLAN (VLAN1), which needs to be assigned to at least one LAN port.

Note the following about VLANs and PVIDs:

- One physical port is assigned to at least one VLAN.
- One physical port can be assigned to multiple VLANs.
- When one port is assigned to multiple VLANs, the port is used as a trunk port to connect to another switch or router.
- When a port receives an untagged packet, this packet is forwarded to a VLAN based on the PVID.
- When a port receives a tagged packet, this packet is forwarded to a VLAN based on the ID that is extracted from the tagged packet.

When you create a VLAN profile, assign LAN ports to the VLAN, and enable the VLAN, the LAN ports that are members of the VLAN can send and receive both tagged and untagged packets. Untagged packets that enter these LAN ports are assigned to the default PVID 1; packets that leave these LAN ports with the same default PVID 1 are untagged. All other packets are tagged according to the VLAN ID that you assigned to the VLAN when you created the VLAN profile.

The following is a typical scenario for a configuration with an IP phone that has two Ethernet ports, one of which is connected to the VPN firewall, the other one to another device:

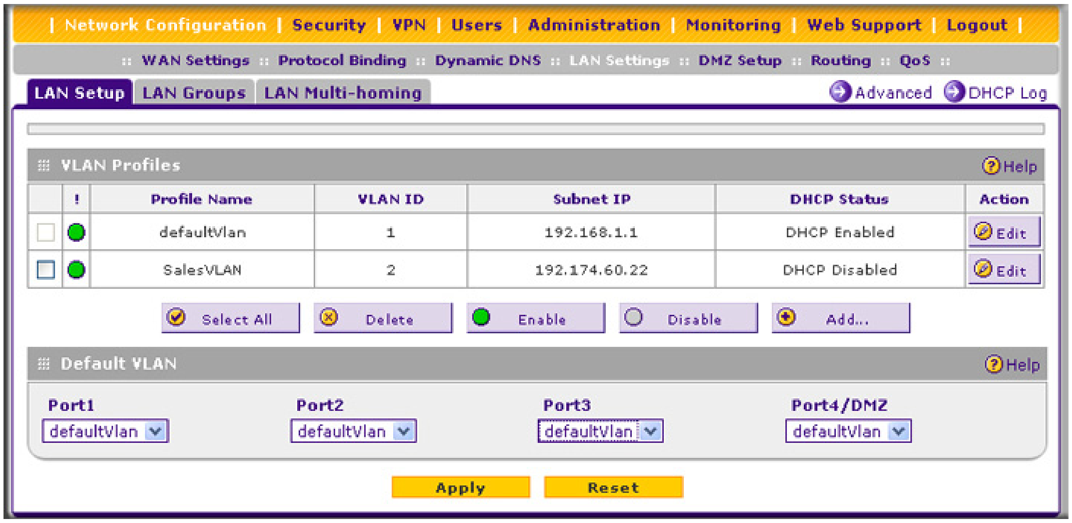
Packets coming from the IP phone to the VPN firewall LAN port are tagged. Packets passing through the IP phone from a connected device to the VPN firewall LAN port are untagged. When you assign the VPN firewall LAN port to a VLAN, packets entering and leaving that LAN port are tagged with the VLAN ID. However, untagged packets entering the VPN firewall

LAN port are forwarded to the default VLAN with PVID 1; packets that leave the LAN port with the same default PVID 1 are untagged.

Assign and Manage VLAN Profiles

➤ **To assign VLAN profiles to the LAN ports and manage VLAN profiles:**

1. Select **Network Configuration > LAN Settings**. The LAN submenu tabs display, with the LAN Setup screen in view. (The following figure shows the default VLAN profile and another VLAN profile as examples.)



VLAN Profiles

	!	Profile Name	VLAN ID	Subnet IP	DHCP Status	Action
☐	●	defaultVlan	1	192.168.1.1	DHCP Enabled	Edit
☐	●	SalesVLAN	2	192.174.60.22	DHCP Disabled	Edit

Default VLAN

Port1	Port2	Port3	Port4/DMZ
defaultVlan	defaultVlan	defaultVlan	defaultVlan

Figure 29.

For each VLAN profile, the following fields are displayed in the VLAN Profiles table:

- **Check box**. Allows you to select the VLAN profile in the table.
- **Status icon**. Indicates the status of the VLAN profile:
  - Green circle. The VLAN profile is enabled.
  - Gray circle. The VLAN profile is disabled.
- **Profile Name**. The unique name assigned to the VLAN profile.
- **VLAN ID**. The unique ID (or tag) assigned to the VLAN profile.
- **Subnet IP**. The subnet IP address for the VLAN profile.
- **DHCP Status**. The DHCP server status for the VLAN profile, which can be either DHCP Enabled or DHCP Disabled.
- **Action**. The Edit table button that provides access to the Edit VLAN Profile screen.

2. Assign a VLAN profile to a LAN port (Port 1, Port 2, Port 3, or Port 4/DMZ) by selecting a VLAN profile from the drop-down list. Both enabled and disabled VLAN profiles are displayed in the drop-down lists.
3. Click **Apply** to save your settings.

Note: For information about how to add and edit a VLAN profile, including its DHCP options, see *Configure a VLAN Profile* on page 59.

VLAN DHCP Options

For each VLAN, you need to specify the Dynamic Host Configuration Protocol (DHCP) options.

DHCP Server

The default VLAN (VLAN 1) has the DHCP Server option enabled by default, allowing the VPN firewall to assign IP, DNS server, WINS server, and default gateway addresses to all computers connected to the VPN firewall’s LAN. The assigned default gateway address is the LAN address of the VPN firewall. IP addresses are assigned to the attached computers from a pool of addresses that you need to specify. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN. When you create a new VLAN, the DHCP server option is disabled by default.

For most applications, the default DHCP server and TCP/IP settings of the VPN firewall are satisfactory.

The VPN firewall delivers the following settings to any LAN device that requests DHCP:

- An IP address from the range that you have defined
- Subnet mask
- Gateway IP address (the VPN firewall’s LAN IP address)
- Primary DNS server (the VPN firewall’s LAN IP address)
- WINS server (if you entered a WINS server address in the DHCP Setup screen)
- Lease time (the date obtained and the duration of the lease)

DHCP Relay

DHCP relay options allow you to make the VPN firewall a DHCP relay agent for a VLAN. The DHCP relay agent makes it possible for DHCP broadcast messages to be sent over routers that do not support forwarding of these types of messages. The DHCP relay agent is therefore the routing protocol that enables DHCP clients to obtain IP addresses from a DHCP server on a remote subnet. If you do not configure a DHCP relay agent for a VLAN, its clients can obtain IP addresses only from a DHCP server that is on the same subnet. To enable clients to obtain IP addresses from a DHCP server on a remote subnet, you need to configure the DHCP relay agent on the subnet that contains the remote clients, so that the DHCP relay agent can relay DHCP broadcast messages to your DHCP server.

DNS Proxy

When the DNS Proxy option is enabled for a VLAN, the VPN firewall acts as a proxy for all DNS requests and communicates with the ISP's DNS servers (as configured on the WAN ISP Settings screens). All DHCP clients receive the primary and secondary DNS IP addresses along with the IP address where the DNS proxy is located (that is, the VPN firewall's LAN IP address). When the DNS Proxy option is disabled for a VLAN, all DHCP clients receive the DNS IP addresses of the ISP but without the DNS proxy IP address. A DNS proxy is particularly useful in auto-rollover mode. For example, if the DNS servers for each WAN connection are different servers, then a link failure might render the DNS servers inaccessible. However, when the DNS Proxy option is enabled, the DHCP clients can make requests to the VPN firewall, which, in turn, can send those requests to the DNS servers of the active WAN connection. However, disable the DNS proxy if you are using a dual-WAN configuration in auto-rollover mode with route diversity (that is, with two different ISPs) and you cannot ensure that the DNS server is available after a rollover has occurred.

LDAP Server

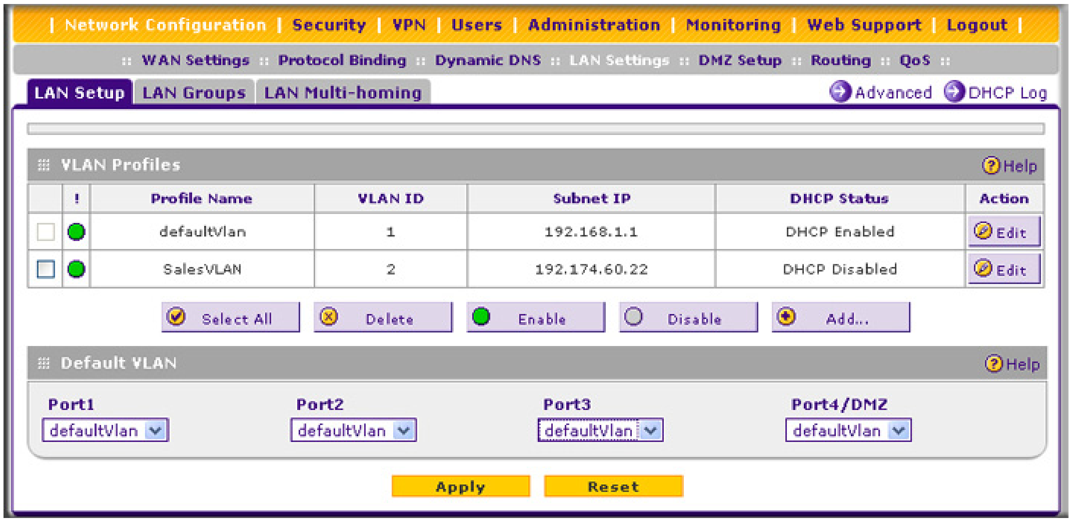
A Lightweight Directory Access Protocol (LDAP) server allows a user to query and modify directory services that run over TCP/IP. For example, clients can query email addresses, contact information, and other service information using an LDAP server. For each VLAN, you can specify an LDAP server and a search base that defines the location in the directory (that is, the directory tree) from which the LDAP search begins.

Configure a VLAN Profile

For each VLAN on the VPN firewall, you can configure its profile, port membership, LAN TCP/IP settings, DHCP options, DNS server, and inter-VLAN routing.

➤ **To add or edit a VLAN profile:**

1. Select **Network Configuration > LAN Settings**. The LAN submenu tabs display, with the LAN Setup screen in view. (The following figure shows the default VLAN profile and another VLAN profile as examples.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
LAN Setup
LAN Groups
LAN Multi-homing
Advanced
DHCP Log
Help
Select All
Delete
Enable
Disable
Add...
Help
Apply
Reset

VLAN Profiles

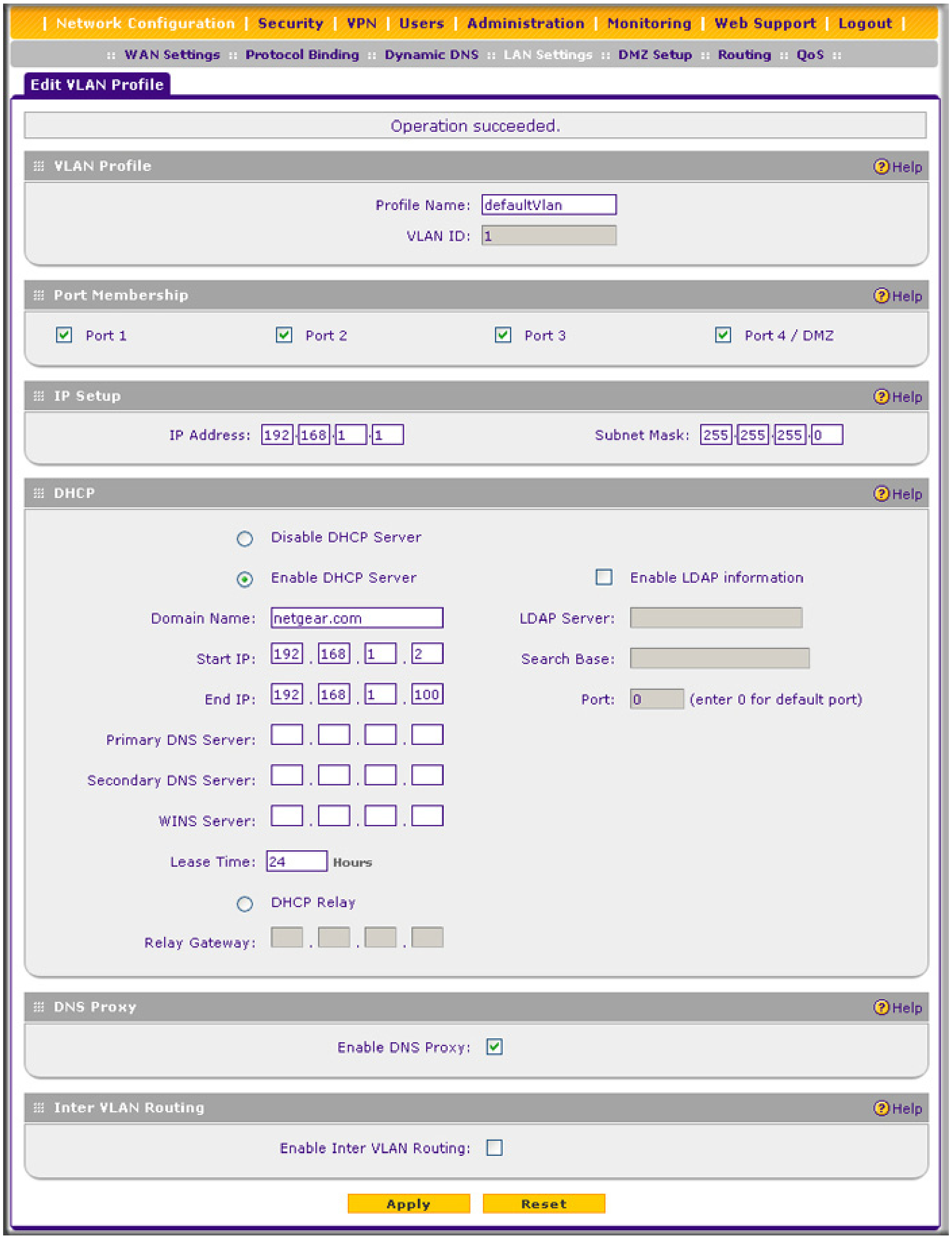
	!	Profile Name	VLAN ID	Subnet IP	DHCP Status	Action
□	●	defaultVlan	1	192.168.1.1	DHCP Enabled	Edit
□	●	SalesVLAN	2	192.174.60.22	DHCP Disabled	Edit

Default VLAN

Port1	Port2	Port3	Port4/DMZ
defaultVlan	defaultVlan	defaultVlan	defaultVlan

Figure 30.

2. Either select an entry from the VLAN Profiles table and click the corresponding **Edit** table button, or add a new VLAN profile by clicking the **Add** table button under the VLAN Profiles table. The Edit VLAN Profile screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
Edit VLAN Profile
Help
Apply
Reset

Operation succeeded.

VLAN Profile

Profile Name: defaultVlan

VLAN ID: 1

Port Membership

☑ Port 1 ☑ Port 2 ☑ Port 3 ☑ Port 4 / DMZ

IP Setup

IP Address: 192 . 168 . 1 . 1 Subnet Mask: 255 . 255 . 255 . 0

DHCP

○ Disable DHCP Server

● Enable DHCP Server □ Enable LDAP information

Domain Name: netgear.com LDAP Server:

Start IP: 192 . 168 . 1 . 2 Search Base:

End IP: 192 . 168 . 1 . 100 Port: 0 (enter 0 for default port)

Primary DNS Server: . . .

Secondary DNS Server: . . .

WINS Server: . . .

Lease Time: 24 Hours

○ DHCP Relay

Relay Gateway: . . .

DNS Proxy

Enable DNS Proxy: ☑

Inter VLAN Routing

Enable Inter VLAN Routing: □

Figure 31.

3. Enter the settings as explained in the following table:

Table 12. Edit VLAN Profile screen settings

Setting	Description
VLAN Profile	
Profile Name	Enter a unique name for the VLAN profile. **Note:** You can also change the profile name of the default VLAN.
VLAN ID	Enter a unique ID number for the VLAN profile. No two VLANs can have the same VLAN ID number. **Note:** You can enter VLAN IDs from 2 to 4093. VLAN ID 1 is reserved for the default VLAN; VLAN ID 4094 is reserved for the DMZ interface.
Port Membership	
Port 1 Port 2 Port 3 Port 4 / DMZ	Select one, several, or all port check boxes to make the ports members of this VLAN. **Note:** A port that is defined as a member of a VLAN profile can send and receive data frames that are tagged with the VLAN ID.
IP Setup	
IP Address	Enter the IP address of the VPN firewall (the factory default is 192.168.1.1). **Note:** Always make sure that the LAN port IP address and DMZ port IP address are in different subnets. **Note:** If you change the LAN IP address of the VLAN while being connected through the browser to the VLAN, you will be disconnected. You then need to open a new connection to the new IP address and log in again. For example, if you change the default IP address 192.168.1.1 to 10.0.0.1, you now need to enter **https://10.0.0.1** in your browser to reconnect to the web management interface.
Subnet Mask	Enter the IP subnet mask. The subnet mask specifies the network number portion of an IP address. Based on the IP address that you assign, the VPN firewall automatically calculates the subnet mask. Unless you are implementing subnetting, use 255.255.255.0 as the subnet mask (computed by the VPN firewall).
DHCP	
Disable DHCP Server	If another device on your network is the DHCP server for the VLAN, or if you will manually configure the network settings of all of your computers, select the **Disable DHCP Server** radio button to disable the DHCP server. This is the default setting.

Table 12. Edit VLAN Profile screen settings (continued)

Setting	Description	
Enable DHCP Server	Select the **Enable DHCP Server** radio button to enable the VPN firewall to function as a Dynamic Host Configuration Protocol (DHCP) server, providing TCP/IP configuration for all computers connected to the VLAN. Enter the following settings.	
	Domain Name	This is optional. Enter the domain name of the VPN firewall.
	Start IP	Enter the starting IP address. This address specifies the first of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address between this address and the ending IP address. The IP address 192.168.1.2 is the default start address.
	End IP	Enter the ending IP address. This address specifies the last of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address between the starting IP address and this IP address. The IP address 192.168.1.100 is the default ending address. **Note:** The starting and ending DHCP IP addresses should be in the same network as the IP address of the VPN firewall (that is, the IP address in the *IP Setup* section of the screen).
	Primary DNS Server	This is optional. If an IP address is specified, the VPN firewall provides this address as the primary DNS server IP address. If no address is specified, the VPN firewall uses the VLAN IP address as the primary DNS server IP address.
	Secondary DNS Server	This is optional. If an IP address is specified, the VPN firewall provides this address as the secondary DNS server IP address.
	WINS Server	This is optional. Enter a WINS server IP address to specify the Windows NetBIOS server, if one is present in your network.
	Lease Time	Enter a lease time. This specifies the duration for which IP addresses are leased to clients.
DHCP Relay	Select the **DHCP Relay** radio button to use the VPN firewall as a DHCP relay agent for a DHCP server somewhere else on your network. Enter the following setting:	
	Relay Gateway	The IP address of the DHCP server for which the VPN firewall serves as a relay.

Table 12. Edit VLAN Profile screen settings (continued)

Setting	Description	
Enable LDAP information	Select the **Enable LDAP information** check box to enable the DHCP server to provide Lightweight Directory Access Protocol (LDAP) server information. Enter the following settings. **Note:** The LDAP settings that you specify as part of the VLAN profile are used only for SSL VPN and VPN firewall authentication, but not for web and email security.	
	LDAP Server	The IP address or name of the LDAP server.
	Search Base	The search objects that specify the location in the directory tree from which the LDAP search begins. You can specify multiple search objects, separated by commas. The search objects include: • cn (for common name) • ou (for organizational unit) • o (for organization) • c (for country) • dc (for domain) For example, to search the Netgear.net domain for all last names of Johnson, you would enter: cn=Johnson,dc=Netgear,dc=net
	Port	The port number for the LDAP server. The default setting is 0 (zero).
DNS Proxy		
Enable DNS Proxy	This is optional. Select the **Enable DNS Proxy** radio button to enable the VPN firewall to provide a LAN IP address for DNS address name resolution. This setting is disabled by default. **Note:** When you deselect the **Enable DNS Proxy** radio button, the VPN firewall still services DNS requests that are sent to its LAN IP address.	
Inter VLAN Routing		
Enable Inter VLAN Routing	This is optional. Select the **Enable Inter VLAN Routing** radio button to ensure that traffic is routed only to VLANs for which inter VLAN routing is enabled. This setting is disabled by default. When the **Enable Inter VLAN Routing** radio button is not selected, traffic from this VLAN is not routed to other VLANs, and traffic from other VLANs is not routed to this VLAN.	

4. Click **Apply** to save your settings.

Note: For information about how to manage VLANs, see *Assign and Manage VLAN Profiles* on page 57.

Note: Once you have completed the LAN setup, all outbound traffic is allowed and all inbound traffic is discarded except responses to requests from the LAN side. For information about how to change these default traffic rules, see *Chapter 4, Firewall Protection*.

Note: For information about the DHCP log, see *View the DHCP Log* on page 288.

➤ **To edit a VLAN profile:**

1. On the LAN Setup screen (see *Figure 30* on page 59), click the **Edit** button in the Action column for the VLAN profile that you want to modify. The Edit VLAN Profile screen displays. This screen is identical to the Add VLAN Profile screen (see the previous screen)
2. Modify the settings as explained in the previous table.
3. Click **Apply** to save your settings.

➤ **To enable, disable, or delete one or more VLAN profiles:**

1. On the LAN Setup screen (see *Figure 30* on page 59), select the check box to the left of the VLAN profile that you want to delete, or click the **Select All** table button to select all profiles. (You cannot select the default VLAN profile.)
2. Click one of the following table buttons:
   - **Enable**. Enables the VLAN or VLANs. The “!” status icon changes from a gray circle to a green circle, indicating that the selected VLAN or VLANs are enabled. (By default, when a VLAN is added to the table, it is automatically enabled.)
   - **Disable**. Disables the VLAN or VLANs. The “!” status icon changes from a green circle to a gray circle, indicating that the selected VLAN or VLANs are disabled.
   - **Delete**. Deletes the VLAN or VLANs.

Configure VLAN MAC Addresses and LAN Advanced Settings

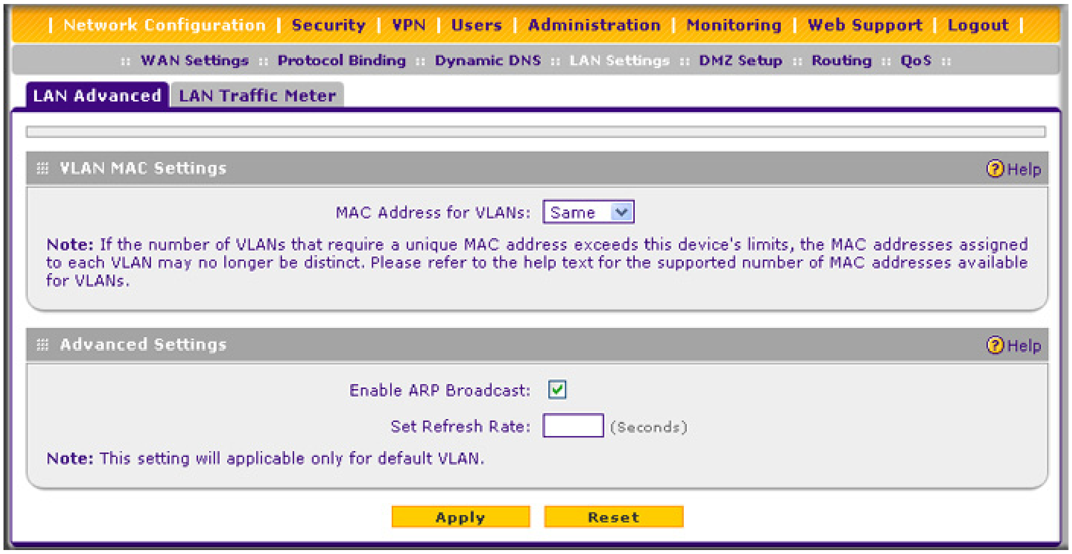
By default, all configured VLAN profiles share the same single MAC address as the LAN ports. (All LAN ports share the same MAC address). However, you can change the VLAN MAC settings to allow up to 16 VLANs to each be assigned a unique MAC address.

You can also enable or disable the broadcast of Address Resolution Protocol (ARP) packets for the default VLAN. If the broadcast of ARP packets is enabled, IP addresses can be mapped to physical addresses (that is, MAC addresses).

For information about the LAN traffic meter, see *Enable the LAN Traffic Meter* on page 266.

➢ **To configure a VLAN to have a unique MAC address:**

1. Select **Network Configuration > LAN Settings**. The LAN submenu tabs display, with the LAN Setup screen in view (see *Figure 30* on page 59).
2. Select the **Advanced** option arrow in the upper right of the LAN Setup screen. The LAN Advanced screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
LAN Advanced
LAN Traffic Meter
VLAN MAC Settings
?Help
Advanced Settings
?Help
Apply
Reset

MAC Address for VLANs: Same

Note: If the number of VLANs that require a unique MAC address exceeds this device's limits, the MAC addresses assigned to each VLAN may no longer be distinct. Please refer to the help text for the supported number of MAC addresses available for VLANs.

Enable ARP Broadcast: ☑

Set Refresh Rate: (Seconds)

Note: This setting will applicable only for default VLAN.

Figure 32.

3. From the MAC Address for VLANs drop-down list, select **Unique**. (The default is Same.)
4. As an option, you can disable the broadcast of ARP packets for the default VLAN by clearing the **Enable ARP Broadcast** check box. (The broadcast of ARP packets is enabled by default for the default VLAN.)
5. Click **Apply** to save your settings.

Note: If you attempt to configure more than 16 VLANs while the MAC address for VLANs is set to Unique on the LAN Advanced screen, the MAC addresses that are assigned to each VLAN might no longer be distinct.

Configure Multi-Home LAN IP Addresses on the Default VLAN

If you have computers using different IP networks in the LAN (for example, 172.16.2.0 or 10.0.0.0), you can add aliases to the LAN ports and give computers on those networks access to the Internet, but you can do so only for the default VLAN. The IP addresses that are assigned as secondary IP addresses need to be unique and should not be assigned to the VLAN.

It is important that you ensure that any secondary LAN addresses are different from the primary LAN, WAN, and DMZ IP addresses and subnet addresses that are already configured on the VPN firewall.The following is an example of correctly configured IP addresses:

WAN1 IP address: 10.0.0.1 with subnet 255.0.0.0
WAN2 IP address: 20.0.0.1 with subnet 255.0.0.0
DMZ IP address: 192.168.10.1 with subnet 255.255.255.0
Primary LAN IP address: 192.168.1.1 with subnet 255.255.255.0
Secondary LAN IP address: 192.168.20.1 with subnet 255.255.255.0

➤ To add a secondary LAN IP address to the default VLAN:

1. Select **Network Configuration > LAN Settings > LAN Multi-homing**. The LAN Multi-homing screen displays:

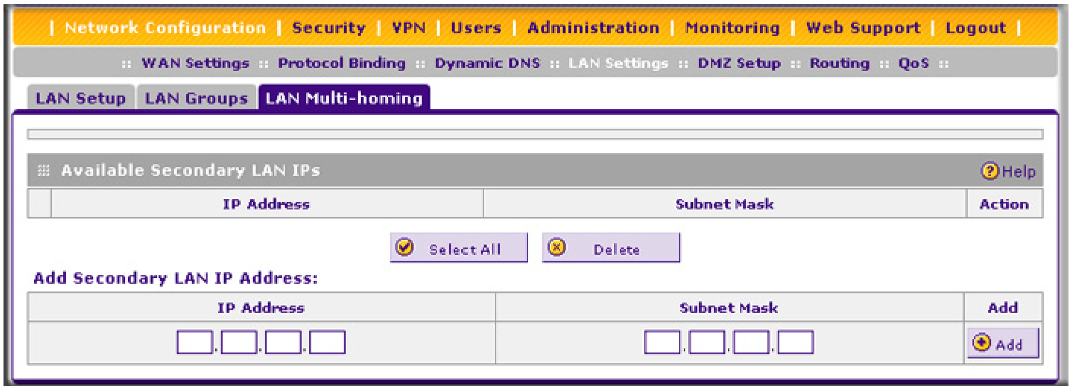

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
LAN Setup
LAN Groups
LAN Multi-homing
Available Secondary LAN IPs
Help
IP Address
Subnet Mask
Action
Select All
Delete
Add Secondary LAN IP Address:
IP Address
Subnet Mask
Add
Add

Figure 33.

The Available Secondary LAN IPs table displays the secondary LAN IP addresses that were added to the VPN firewall.

2. In the Add Secondary LAN IP Address section of the screen, enter the following settings:
   - **IP Address**. Enter the secondary address that you want to assign to the LAN ports.
   - **Subnet Mask**. Enter the subnet mask for the secondary IP address.
3. Click the **Add** table button in the rightmost column to add the secondary IP address to the Available Secondary LAN IPs table.

   Repeat *step 2* and *step 3* for each secondary IP address that you want to add to the Available Secondary LAN IPs table.

Note: Secondary IP addresses cannot be configured on the DHCP server. The hosts on the secondary subnets needs to be manually configured with the IP addresses, gateway IP address, and DNS server IP addresses.

➤ **To edit a secondary LAN IP address:**

1. On the LAN Multi-homing screen (see the previous screen), click the **Edit** button in the Action column for the secondary IP address that you want to modify. The Edit Secondary LAN IP address screen displays.
2. Modify the IP address or subnet mask, or both.
3. Click **Apply** to save your settings.

➤ **To delete one or more secondary LAN IP addresses:**

1. On the LAN Multi-homing screen (see the previous screen), select the check box to the left of the secondary IP address that you want to delete, or click the **Select All** table button to select secondary IP addresses.
2. Click the **Delete** table button.

Manage Groups and Hosts (LAN Groups)

The Known PCs and Devices table on the LAN Groups screen (see *Figure 34* on page 68) contains a list of all known PCs and network devices that are assigned dynamic IP addresses by the VPN firewall, or have been discovered by other means. Collectively, these entries make up the network database.

The network database is updated by these three methods:

- **DHCP client requests**. When the DHCP server is enabled, it accepts and responds to DHCP client requests from PCs and other network devices. These requests also generate an entry in the network database. This is an advantage of enabling the DHCP Server feature.
- **Scanning the network**. The local network is scanned using Address Resolution Protocol (ARP) requests. The ARP scan detects active devices that are not DHCP clients.

Note: In large networks, scanning the network might generate unwanted traffic.

Note: When the VPN firewall receives a reply to an ARP request, it might not be able to determine the device name if the software firewall of the device blocks the name.

- **Manual entry**. You can manually enter information about a network device.

Some advantages of the network database are:

- Generally, you do not need to enter either IP address or MAC addresses. Instead, you can just select the name of the desired PC or device.

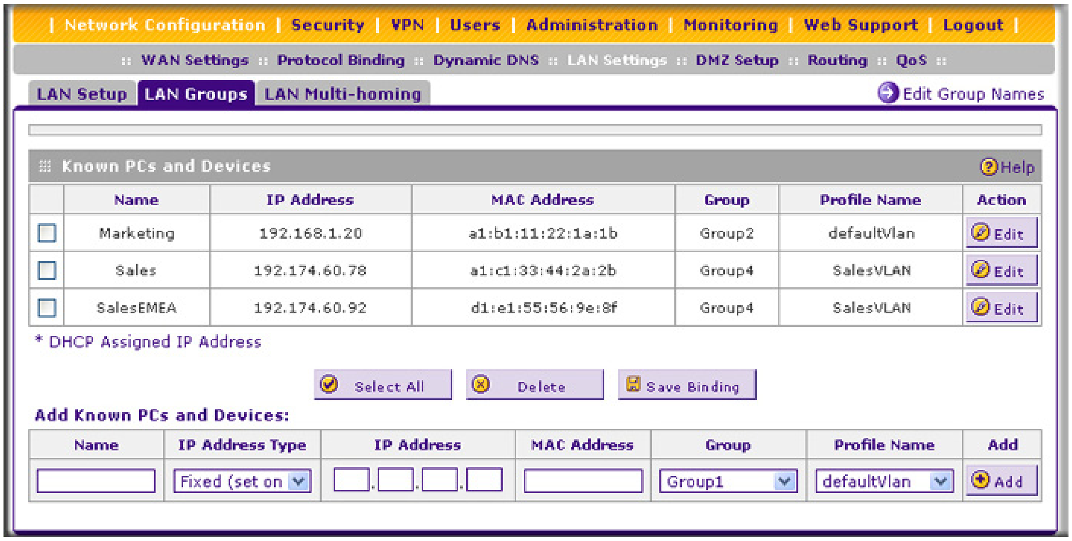
- There is no need to reserve an IP address for a PC in the DHCP server. All IP address assignments made by the DHCP server are maintained until the PC or device is removed from the network database, either by expiration (inactive for a long time) or by you.
- There is no need to use a fixed IP address on a PCs. Because the IP address allocated by the DHCP server never changes, you do not need to assign a fixed IP address to a PC to ensure that it always has the same IP address.
- A PC is identified by its MAC address—not by its IP address. The network database uses the MAC address to identify each PC or device. Therefore, changing a PC's IP address does not affect any restrictions applied to that PC.
- Control over PCs can be assigned to groups and individuals:
  - You can assign PCs to groups (see *Manage the Network Database* on page 68 on this page) and apply restrictions (LAN WAN outbound rules, LAN DMZ outbound rules, LAN WAN inbound rules, and LAN DMZ inbound rules) to each group (see *Use Rules to Block or Allow Specific Kinds of Traffic* on page 82).
  - If necessary, you can also create firewall rules to apply to a single PC (see *Enable Source MAC Filtering* on page 126). Because the MAC address is used to identify each PC, users cannot avoid these restrictions by changing their IP address.

Manage the Network Database

You can view the network database, manually add or remove database entries, and edit database entries.

➢ **To view the network database:**

1. Select **Network Configuration > LAN Settings > LAN Groups**. The LAN Groups screen displays. (The following figure shows some examples in the Known PCs and Devices table.)



| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
LAN Setup
LAN Groups
LAN Multi-homing
Edit Group Names

Known PCs and Devices

	Name	IP Address	MAC Address	Group	Profile Name	Action
□	Marketing	192.168.1.20	a1:b1:11:22:1a:1b	Group2	defaultVlan	Edit
□	Sales	192.174.60.78	a1:c1:33:44:2a:2b	Group4	SalesVLAN	Edit
□	SalesEMEA	192.174.60.92	d1:e1:55:56:9e:8f	Group4	SalesVLAN	Edit

* DHCP Assigned IP Address

Select All
Delete
Save Binding

Add Known PCs and Devices:

Name	IP Address Type	IP Address	MAC Address	Group	Profile Name	Add
	Fixed (set on	. . .		Group1	defaultVlan	Add

Figure 34.

The Known PCs and Devices table lists the entries in the network database. For each PC or device, the following fields are displayed:

- **Check box**. Allows you to select the PC or device in the table.
- **Name**. The name of the PC or device. For computers that do not support the NetBIOS protocol, the name is displayed as Unknown (you can edit the entry manually to add a meaningful name). If the PC or device was assigned an IP address by the DHCP server, then the name is appended by an asterisk.
- **IP Address**. The current IP address of the PC or device. For DHCP clients of the VPN firewall, this IP address does not change. If a PC or device is assigned a static IP address, you need to update this entry manually after the IP address on the PC or device has changed.
- **MAC Address**. The MAC address of the PC or device’s network interface.
- **Group**. Each PC or device can be assigned to a single LAN group. By default, a PC or device is assigned to Group 1. You can select a different LAN group from the Group drop-down list in the Add Known PCs and Devices section or on the Edit Groups and Hosts screen.
- **Profile Name**. The VLAN to which the PC or device is assigned.
- **Action**. The Edit table button that provides access to the Edit Groups and Hosts screen.

Add PCs or Devices to the Network Database

➢ To add PCs or devices manually to the network database:

1. In the Add Known PCs and Devices section of the LAN Groups screen (see *Figure 34* on page 68), enter the settings as explained in the following table:

Table 13. Known PCs and devices settings

Setting	Description
Name	Enter the name of the PC or device.
IP Address Type	From the drop-down list, select how the PC or device receives it IP address: • **Fixed (set on PC)**. The IP address is statically assigned on the PC or device. • **Reserved (DHCP Client)**. Directs the VPN firewall’s DHCP server to always assign the specified IP address to this client during the DHCP negotiation (see *Set Up Address Reservation* on page 72). **Note:** When assigning a reserved IP address to a client, the IP address selected needs to be outside the range of addresses allocated to the DHCP server pool.
IP Address	Enter the IP address that this PC or device is assigned in the IP Address field. If the IP address type is Reserved (DHCP Client), the VPN firewall reserves the IP address for the associated MAC address.

Table 13. Known PCs and devices settings (continued)

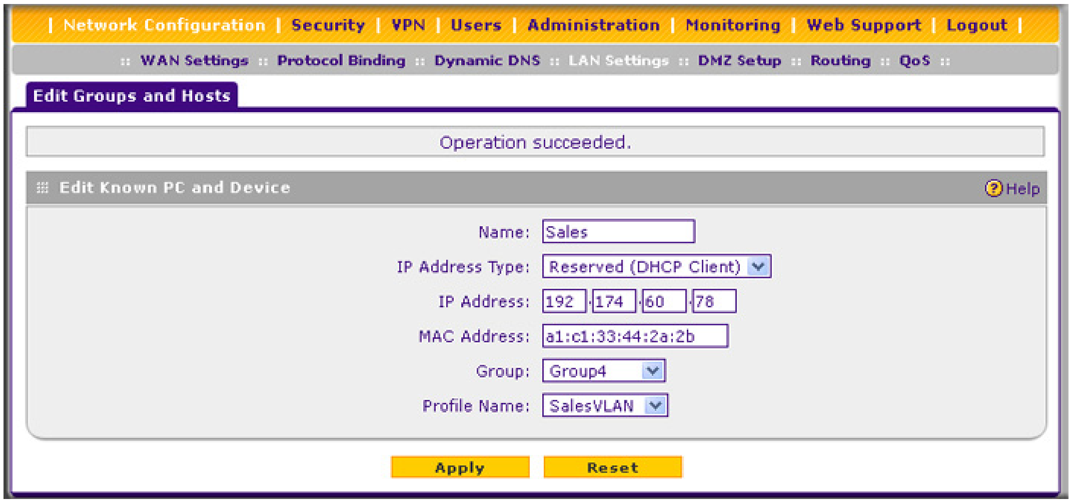
Setting	Description
MAC Address	Enter the MAC address of the PC or device’s network interface. The MAC address format is six colon-separated pairs of hexadecimal characters (0–9 and A–F), such as 01:23:45:67:89:AB.
Group	From the drop-down list, select the group to which the PC or device is assigned. (Group 1 is the default group.)
Profile Name	From the drop-down list, select the VLAN profile to which the PC or device is assigned. (defaultVlan is the default VLAN group.)

2. Click the **Add** table button to add the PC or device to the Known PCs and Devices table.
3. As an optional step: To enable DHCP address reservation for the entry that you just added to the Known PCs and Devices table, select the check box for the table entry and click **Save Binding** to bind the IP address to the MAC address for DHCP assignment.

Edit PCs or Devices in the Network Database

➤ **To edit PCs or devices manually in the network database:**

1. In the Known PCs and Devices table of the LAN Groups screen (see *Figure 34* on page 68), click the **Edit** table button of a table entry. The Edit Groups and Hosts screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
Edit Groups and Hosts
Help
Apply
Reset

Operation succeeded.

Edit Known PC and Device

Name: Sales

IP Address Type: Reserved (DHCP Client)

IP Address: 192 .174 .60 .78

MAC Address: a1:c1:33:44:2a:2b

Group: Group4

Profile Name: SalesVLAN

Figure 35.

2. In the Edit Known PC and Device section, modify the settings as explained in *Table 13* on page 69.
3. Click **Apply** to save your settings in the Known PCs and Devices table.

Deleting PCs or Devices from the Network Database

➢ **To delete one or more PCs or devices from the network database:**

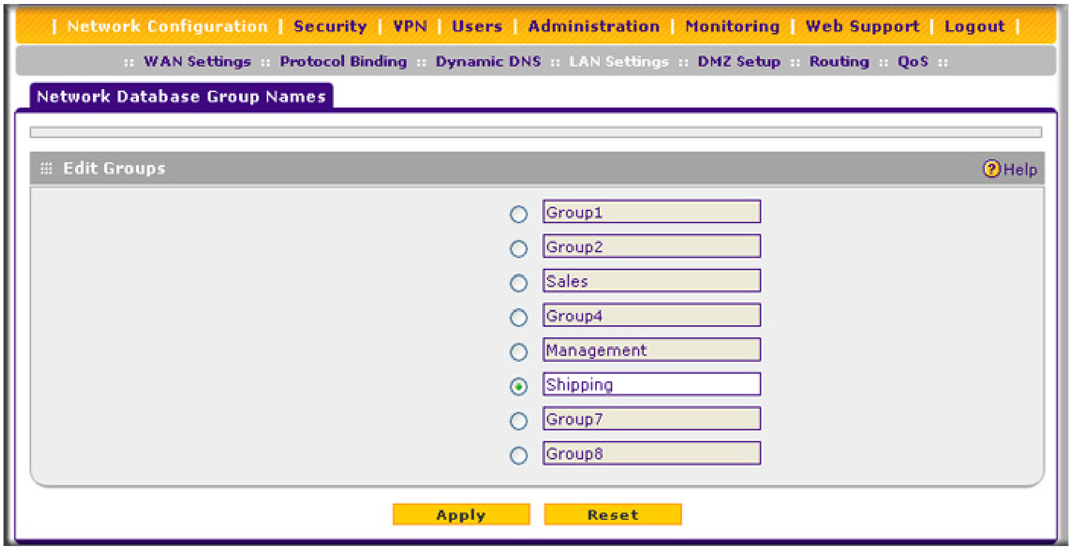
1. On the LAN Groups screen (see *Figure 34* on page 68), select the check box to the left of the PC or device that you want to delete, or click the **Select All** table button to select all PCs and devices.
2. Click the **Delete** table button.

Change Group Names in the Network Database

By default, the groups are named Group1 through Group8. You can rename these group names to be more descriptive, such as GlobalMarketing and GlobalSales.

➢ **To edit the names of any of the eight available groups:**

1. Select **Network Configuration > LAN Settings > LAN Groups**. The LAN Groups screen displays (see *Figure 34* on page 68, which shows some examples in the Known PCs and Devices table).
2. Click the **Edit Group Names** option arrow in the upper right of the LAN Groups screen. The Network Database Group Names screen displays. (The following figure shows some examples.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
Network Database Group Names
Edit Groups
Help
Apply
Reset

○ Group1
○ Group2
○ Sales
○ Group4
○ Management
● Shipping
○ Group7
○ Group8

Figure 36.

3. Select the radio button next to any group name to enable editing.
4. Type a new name in the field. The maximum number of characters is 15; spaces and double quotes (") are not allowed.
5. Repeat *step 3* and *step 4* for any other group names.
6. Click **Apply** to save your settings.

Set Up Address Reservation

When you specify a reserved IP address for a PC or device on the LAN (based on the MAC address of the device), that PC or device always receives the same IP address each time it accesses the VPN firewall's DHCP server. Reserved IP addresses should be assigned to servers or access points that require permanent IP address settings. The reserved IP address that you select need to be outside of the DHCP server pool.

To reserve an IP address, select **Reserved (DHCP Client)** from the IP Address Type drop-down list on the LAN Groups screen as described in *Add PCs or Devices to the Network Database* on page 69 or on the Edit Groups and Hosts screen as described in *Edit PCs or Devices in the Network Database* on page 70.

Note: The reserved address is not assigned until the next time the PC or device contacts the VPN firewall's DHCP server. Reboot the PC or device, or access its IP configuration and force a DHCP release and renew.

Configure and Enable the DMZ Port

The demilitarized zone (DMZ) is a network that, by default, has fewer firewall restrictions when compared to the LAN. The DMZ can be used to host servers (such as a web server, FTP server, or email server) and provide public access to them. The fourth LAN port on the VPN firewall (the rightmost LAN port) can be dedicated as a hardware DMZ port to safely provide services to the Internet without compromising security on your LAN. By default, the DMZ port and both inbound and outbound DMZ traffic are disabled. Enabling the DMZ port and allowing traffic to and from the DMZ increases the traffic through the WAN ports.

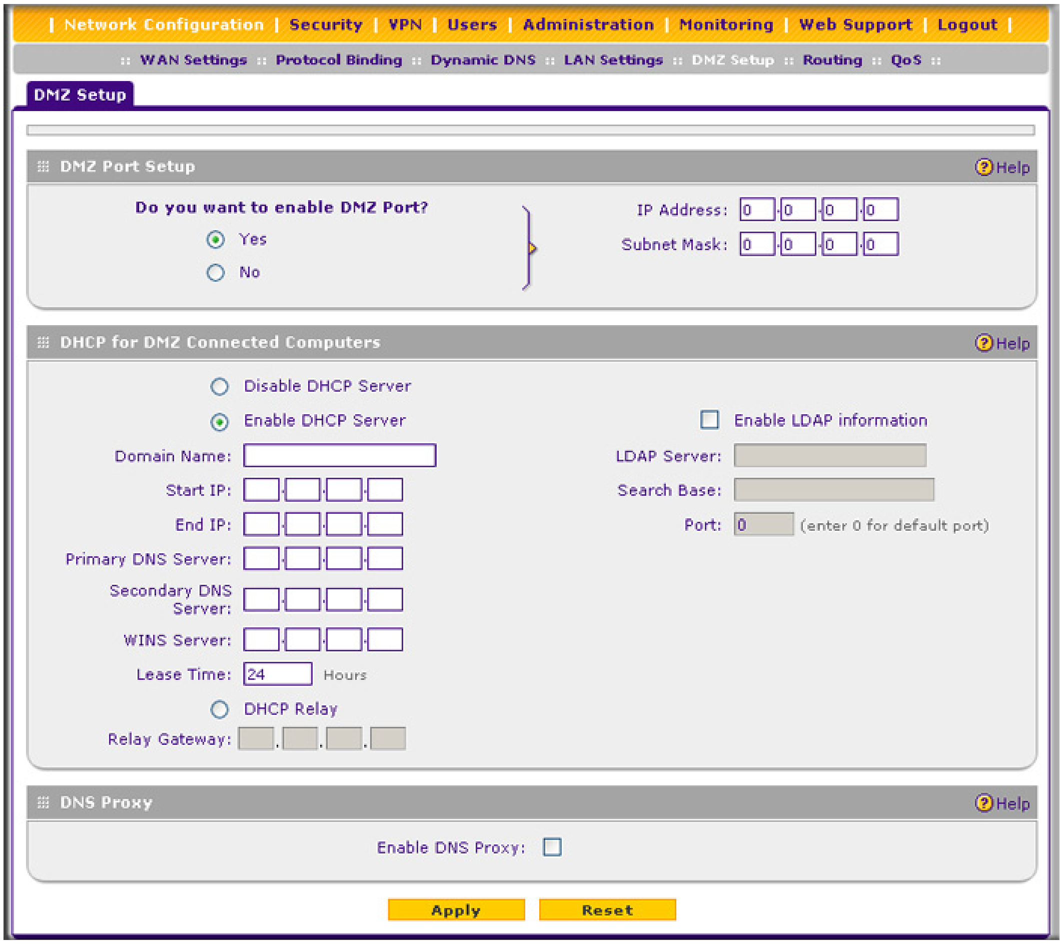
Using a DMZ port is also helpful with online games and videoconferencing applications that are incompatible with NAT. The VPN firewall is programmed to recognize some of these applications and to work correctly with them, but there are other applications that might not function well. In some cases, local PCs can run the application correctly if those PCs are used on the DMZ port.

Note: A separate firewall security profile is provided for the DMZ port that is also physically independent of the standard firewall security component that is used for the LAN.

The DMZ Setup screen lets you set up the DMZ port. It permits you to enable or disable the hardware DMZ port (LAN port 4, see *Front Panel* on page 14) and configure an IP address and subnet mask for the DMZ port.

➢ To enable and configure the DMZ port:

1. Select **Network Configuration > DMZ Setup**. The DMZ Setup screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
DMZ Setup
Help
Apply
Reset

DMZ Port Setup

Do you want to enable DMZ Port?

● Yes

○ No

IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

DHCP for DMZ Connected Computers

○ Disable DHCP Server

● Enable DHCP Server

Domain Name:

Start IP:

End IP:

Primary DNS Server:

Secondary DNS Server:

WINS Server:

Lease Time: 24 Hours

○ DHCP Relay

Relay Gateway:

□ Enable LDAP information

LDAP Server:

Search Base:

Port: 0 (enter 0 for default port)

DNS Proxy

Enable DNS Proxy: □

Figure 37.

2. Enter the settings as explained in the following table:

Table 14. DMZ Setup screen settings

Setting	Description	
DMZ Port Setup		
Do you want to enable DMZ Port?	Select one of the following radio buttons: • **Yes**. Enables you to configure the DMZ port settings. Fill in the IP Address and Subnet Mask fields. • **No**. Allows you to disable the DMZ port after you have configured it.	
	IP Address	Enter the IP address of the DMZ port. Make sure that the DMZ port IP address and LAN port IP address are in different subnets (for example, an address outside the LAN address pool, such as 192.168.1.101).
	Subnet Mask	Enter the IP subnet mask of the DMZ port. The subnet mask specifies the network number portion of an IP address.

Table 14. DMZ Setup screen settings (continued)

Setting	Description	
DHCP		
Disable DHCP Server	If another device on your network is the DHCP server for the VLAN, or if you will manually configure the network settings of all of your computers, select the **Disable DHCP Server** radio button to disable the DHCP server. This is the default setting.	
Enable DHCP Server	Select the **Enable DHCP Server** radio button to enable the VPN firewall to function as a Dynamic Host Configuration Protocol (DHCP) server, providing TCP/IP configuration for all computers connected to the VLAN. Enter the following settings:	
	Domain Name	This is optional. Enter the domain name of the VPN firewall.
	Start IP	Enter the starting IP address. This address specifies the first of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address between this address and the ending IP address. The IP address 192.168.1.2 is the default start address.
	End IP	Enter the ending IP address. This address specifies the last of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address between the starting IP address and this IP address. The IP address 192.168.1.100 is the default ending address. **Note:** The starting and ending DHCP IP addresses should be in the same network as the IP address of the DMZ port (that is, the IP address in the *DMZ Port Setup* section of the screen).
	Primary DNS Server	This is optional. If an IP address is specified, the VPN firewall provides this address as the primary DNS server IP address. If no address is specified, the VPN firewall provides its own LAN IP address as the primary DNS server IP address.
	Secondary DNS Server	This is optional. If an IP address is specified, the VPN firewall provides this address as the secondary DNS server IP address.
	WINS Server	This is optional. Enter a WINS server IP address to specify the Windows NetBIOS server, if one is present in your network.
	Lease Time	Enter a lease time. This specifies the duration for which IP addresses are leased to clients.
DHCP Relay	Select the **DHCP Relay** radio button to use the VPN firewall as a DHCP relay agent for a DHCP server somewhere else on your network. Enter the following setting:	
	Relay Gateway	The IP address of the DHCP server for which the VPN firewall serves as a relay.

Table 14. DMZ Setup screen settings (continued)

Setting	Description	
Enable LDAP information	Select the **Enable LDAP information** check box to enable the DHCP server to provide Lightweight Directory Access Protocol (LDAP) server information. Enter the following settings:	
	LDAP Server	The IP address or name of the LDAP server.
	Search Base	The search objects that specify the location in the directory tree from which the LDAP search begin. You can specify multiple search objects, separated by commas. The search objects include: • cn (for common name) • ou (for organizational unit) • o (for organization) • c (for country) • dc (for domain) For example, to search the Netgear.net domain for all last names of Johnson, you would enter: cn=Johnson,dc=Netgear,dc=net
	Port	The port number for the LDAP server. The default setting is 0 (zero).
DNS Proxy		
Enable DNS Proxy	This is optional. Select the **Enable DNS Proxy** radio button to enable the VPN firewall to provide a LAN IP address for DNS address name resolution. This setting is enabled by default.	

3. Click **Apply** to save your settings.

Note: The DMZ LED next to LAN port 4 (see *Front Panel* on page 14) lights green to indicate that the DMZ port is enabled.

For information about how to define the DMZ WAN rules and LAN DMZ rules, see *Set DMZ WAN Rules* on page 95 and *Set LAN DMZ Rules* on page 98, respectively.

Manage Routing

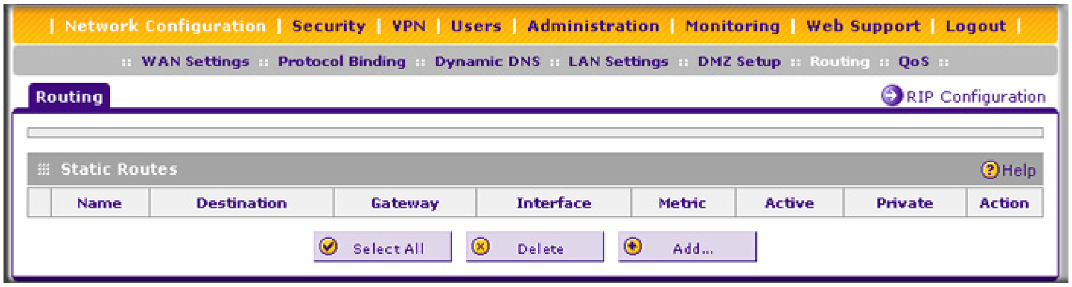
Static routes provide additional routing information to your VPN firewall. Under normal circumstances, the VPN firewall has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You should configure static routes only for unusual cases such as multiple firewalls or multiple IP subnets located on your network.

Note: The VPN firewall automatically sets up routes between VLANs and secondary IP addresses that you have configured on the LAN Multi-homing screen (see *Configure Multi-Home LAN IP Addresses on the Default VLAN* on page 65). Therefore, you do not need to manually add a static route between a VLAN and a secondary IP address.

Configure Static Routes

➢ To add a static route to the Static Routes table:

1. Select **Network Configuration > Routing**. The Routing screen display:

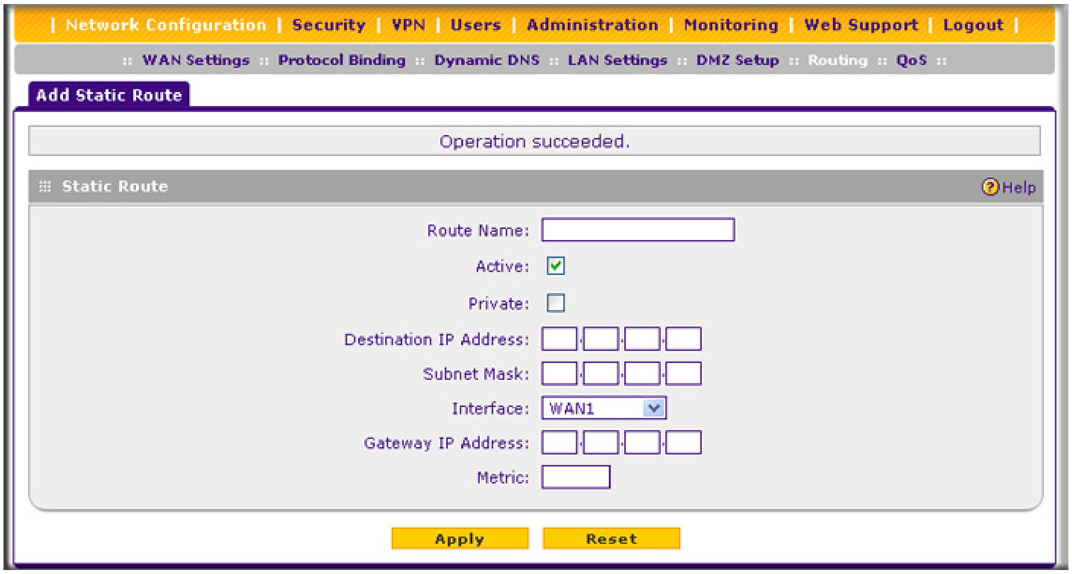

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
Routing
RIP Configuration
Static Routes
Help
Select All
Delete
Add...

	Name	Destination	Gateway	Interface	Metric	Active	Private	Action

Figure 38.

For information about the fields of the Static Routes table, see the following table.

2. Click the **Add** table button under the Static Routes table. The Add Static Route screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
Add Static Route
Static Route
Help
Apply
Reset

Operation succeeded.

Route Name:

Active: ☑

Private: ☐

Destination IP Address: . . .

Subnet Mask: . . .

Interface: WAN1

Gateway IP Address: . . .

Metric:

Figure 39.

3. Enter the settings as explained in the following table:

Table 15. Add Static Route screen settings

Setting	Description
Route Name	The route name for the static route (for purposes of identification and management).
Active	To make the static route effective, select the **Active** check box. **Note:** A route can be added to the table and made inactive, if not needed. This allows routes to be used as needed without deleting and re-adding the entry. an inactive route is not advertised if RIP is enabled.
Private	If you want to limit access to the LAN only, select the **Private** check box. Doing so prevents the static route from being advertised in RIP.
Destination IP Address	The destination IP address of the host or network to which the route leads.
Subnet Mask	The IP subnet mask of the host or network to which the route leads. If the destination is a single host, enter **255.255.255.255**.
Interface	From the drop-down list, select the interface that is the physical network interface (WAN1, WAN2, WAN3, WAN4, or DMZ) or virtual interface (VLAN profile) through which the route is accessible.
Gateway IP Address	The gateway IP address through which the destination host or network can be reached.
Metric	The priority of the route. Select a value between 2 and 15. If multiple routes to the same destination exist, the route with the lowest metric is used.

4. Click **Apply** to save your settings. The new static route is added to the Static Routes table.

➢ To edit a static route that is in the Static Routes table:

1. On the Routing screen (see *Figure 39* on page 76), click the **Edit** button in the Action column for the route that you want to modify. The Edit Static Route screen displays. This screen is identical to the Add Static Route screen (see the previous screen).
2. Modify the settings as explained in the previous table.
3. Click **Apply** to save your settings.

➢ To delete one or more routes:

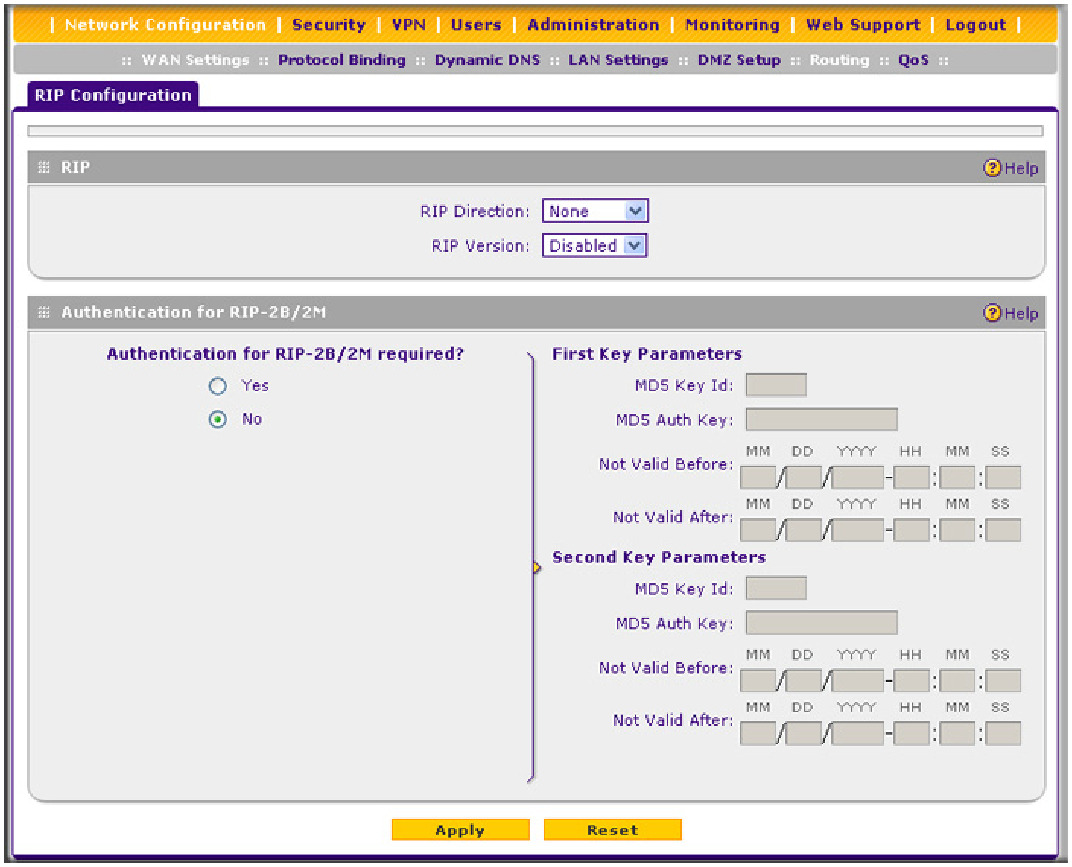
1. On the Routing screen (see *Figure 39* on page 76), select the check box to the left of the route that you want to delete, or click the **Select All** table button to select all routes.
2. Click the **Delete** table button.

Configure Routing Information Protocol

Routing Information Protocol (RIP), RFC 2453, is an Interior Gateway Protocol (IGP) that is commonly used in internal networks (LANs). RIP enables a router to exchange its routing information automatically with other routers, to dynamically adjust its routing tables, and to adapt to changes in the network. RIP is disabled by default.

➤ To enable and configure RIP:

1. Select **Network Configuration > Routing**.
2. Click the **RIP Configuration** option arrow in the upper right of the Routing screen. The RIP Configuration screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
RIP Configuration
Help
Help
Apply
Reset

RIP

RIP Direction: None

RIP Version: Disabled

Authentication for RIP-2B/2M

Authentication for RIP-2B/2M required?

○ Yes

● No

First Key Parameters

MD5 Key Id:

MD5 Auth Key:

Not Valid Before: MM / DD / YYYY - HH : MM : SS

Not Valid After: MM / DD / YYYY - HH : MM : SS

Second Key Parameters

MD5 Key Id:

MD5 Auth Key:

Not Valid Before: MM / DD / YYYY - HH : MM : SS

Not Valid After: MM / DD / YYYY - HH : MM : SS

Figure 40.

3. Enter the settings as explained in the following table:

Table 16. RIP Configuration screen settings

Setting	Description	
RIP		
RIP Direction	From the RIP Direction drop-down list, select the direction in which the VPN firewall sends and receives RIP packets: • **None**. The VPN firewall neither advertises its route table, nor does it accept any RIP packets from other routers. This effectively disables RIP. • **In Only**. The VPN firewall accepts RIP information from other routers but does not advertises its routing table. • **Out Only**. The VPN firewall advertises its routing table but does not accept RIP information from other routers. • **Both**. The VPN firewall advertises its routing table and also processes RIP information received from other routers.	
RIP Version	From the RIP Version drop-down list, select the version: • **Disabled**. The RIP version is disabled. This is the default setting. • **RIP-1**. Classful routing that does not include subnet information. This is the most commonly supported version. • **RIP-2B**. Routing that sends the routing data in RIP-2 format and uses subnet broadcasting. • **RIP-2M**. Routing that sends the routing data in RIP-2 format and uses multicasting.	
Authentication for RIP-2B/2M		
Authentication for RIP-2B/2M required?	Authentication for RP-2B or RIP-2M is disabled by default, that is, the **No** radio button is selected. To enable authentication for RP-2B or RIP-2M, select the **Yes** radio button and enter the settings for the following fields.	
	First Key Parameters	
	MD5 Key Id	The identifier for the key that is used for authentication.
	MD5 Auth Key	The password that is used for MD5 authentication.
	Not Valid Before	The beginning of the lifetime of the MD5 key. Enter the month, date, year, hour, minute, and second. Before this date and time, the MD5 key is not valid.
	Not Valid After	The end of the lifetime of the MD5 key. Enter the month, date, year, hour, minute, and second. After this date and time, the MD5 key is no longer valid.
	Second Key Parameters	
	MD5 Key Id	The identifier for the key that is used for authentication.
	MD5 Auth Key	The password that is used for MD5 authentication.

Table 16. RIP Configuration screen settings (continued)

Setting	Description	
Authentication for RIP-2B/2M required? (continued)	Not Valid Before	The beginning of the lifetime of the MD5 key. Enter the month, date, year, hour, minute, and second. Before this date and time, the MD5 key is not valid.
	Not Valid After	The end of the lifetime of the MD5 key. Enter the month, date, year, hour, minute, and second. After this date and time, the MD5 key is no longer valid.

4. Click **Apply** to save your settings.

Static Route Example

In this example, we assume the following:

- The VPN firewall’s primary Internet access is through a cable modem to an ISP.
- The VPN firewall is on a local LAN with IP address is 192.168.1.100.
- The VPN firewall connects to a remote network where you need to access a device.
- The LAN IP address of the remote network is 134.177.0.0.

When you first configured the VPN firewall, two implicit static routes were created:

- A default static route was created with your ISP as the gateway.
- A second static route was created to the local LAN for all 192.168.1.x addresses.

With this configuration, if you attempt to access a device on the 134.177.0.0 remote network, the VPN firewall forwards your request to the ISP. In turn, the ISP forwards your request to the remote network, where the request is likely to be denied by the remote network’s firewall.

In this case you need to define a static route, informing the VPN firewall that the 134.177.0.0 IP address should be accessed through the local LAN IP address (192.168.1.100).

The static route on the VPN firewall needs to be defined as follows:

- The destination IP address and IP subnet mask need to specify that the static route applies to all 134.177.x.x IP addresses.
- The gateway IP address needs to specify that all traffic for the 134.177.x.x IP addresses should be forwarded to the local LAN IP address (192.168.1.100).
- A metric value of 1 should work since the VPN firewall is on the local LAN.
- The static route can be made private only as a precautionary security measure in case RIP is activated.

Firewall Protection

4

This chapter describes how to use the firewall features of the VPN firewall to protect your network. This chapter contains the following sections:

About Firewall Protection

A firewall protects one network (the trusted network, such as your LAN) from another (the untrusted network, such as the Internet), while allowing communication between the two. You can further segment keyword blocking to certain known groups. For information about how to set up LAN groups, see *Manage Groups and Hosts (LAN Groups)* on page 67.

A firewall incorporates the functions of a Network Address Translation (NAT) router, protects the trusted network from hacker intrusions or attacks, and controls the types of traffic that can flow between the two networks. Unlike simple Internet-sharing NAT routers, a firewall uses a process called stateful packet inspection to protect your network from attacks and intrusions. NAT performs a very limited stateful inspection in that it considers whether the incoming packet is in response to an outgoing request, but true stateful packet inspection goes far beyond NAT.

Administrator Tips

Consider the following operational items:

1. As an option, you can enable remote management if you have to manage distant sites from a central location (see *Configure VPN Authentication Domains, Groups, and Users* on page 219 and *Configure Remote Management Access* on page 250).
2. Although using rules (see *Use Rules to Block or Allow Specific Kinds of Traffic* on page 82) is the basic way of managing the traffic through your system, you can further refine your control using the following features and capabilities of the VPN firewall:
   - Groups and hosts (see *Manage Groups and Hosts (LAN Groups)* on page 67)
   - Services (see *Services-Based Rules* on page 83)
   - Schedules (see *Set a Schedule to Block or Allow Specific Traffic* on page 121)
   - Source MAC filtering (see *Enable Source MAC Filtering* on page 126)
   - Port triggering (see *Configure Port Triggering* on page 130)
3. Some firewall settings might affect the performance of the VPN firewall. For more information, see *Performance Management* on page 242.
4. The firewall logs can be configured to log and then email dropped packet information and other information to a specified email address. For information about how to configure logging and notifications, see *Activate Notification of Events, Alerts, and Syslogs* on page 269.

Use Rules to Block or Allow Specific Kinds of Traffic

Firewall rules are used to block or allow specific traffic passing through from one side to the other. You can configure up to 600 rules on the VPN firewall. Inbound rules (WAN to LAN) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Outbound rules (LAN to WAN) determine what outside resources local users can have access to.

A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the VPN firewall are:

- **Inbound**. Block all access from outside except responses to requests from the LAN side.
- **Outbound**. Allow all access from the LAN side to the outside.

The firewall rules for blocking and allowing traffic on the VPN firewall can be applied to a combination of LAN-WAN traffic, DMZ-WAN traffic, and LAN-DMZ traffic.

Table 17. Number of supported firewall rule configurations

Traffic rule	Maximum number of outbound rules	Maximum number of inbound rules	Maximum number of supported rules
LAN WAN	200	200	200
DMZ WAN	200	200	200

Table 17. Number of supported firewall rule configurations (continued)

Traffic rule	Maximum number of outbound rules	Maximum number of inbound rules	Maximum number of supported rules
LAN DMZ	200	200	200
Maximum Number of Supported Rules	300	300	600

The maximum number of supported outbound rules is 300, and the maximum number of supported inbound rules is 300. The total number of supported inbound and outbound rules is therefore 600.

Per traffic rule category (LAN WAN, DMZ WAN, or LAN DMZ), you can configure a total of 200 rules in any combination of outbound and inbound rules. However, the maximum number of outbound rules for all three categories cannot exceed 300. Similarly, the maximum number of inbound rules for all three categories cannot exceed 300.

Services-Based Rules

The rules to block traffic are based on the traffic's category of service:

- **Outbound rules (service blocking)**. Outbound traffic is normally allowed unless the firewall is configured to disallow it.
- **Inbound rules (port forwarding)**. Inbound traffic is normally blocked by the firewall unless the traffic is in response to a request from the LAN side. The firewall can be configured to allow this otherwise blocked traffic.
- **Customized services**. Additional services can be added to the list of services in the factory default list. These added services can then have rules defined for them to either allow or block that traffic (see *Add Customized Services* on page 112).
- **Quality of Service (QoS) priorities**. Each service has its own native priority that impacts its quality of performance and tolerance for jitter or delays. You can change the QoS priority, which changes the traffic mix through the system (see *Create Quality of Service (QoS) Profiles* on page 116).

Outbound Rules (Service Blocking)

The VPN firewall allows you to block the use of certain Internet services by PCs on your network. This is called service blocking or port filtering.

Note: See *Enable Source MAC Filtering* on page 126 for yet another way to block outbound traffic from selected PCs that would otherwise be allowed by the firewall.

WARNING!

Allowing inbound services opens security holes in your VPN firewall. Enable only those ports that are necessary for your network.

The following table describes the fields that define the rules for outbound traffic and that are common to most Outbound Service screens (see *Figure 43* on page 93, *Figure 46* on page 96, and *Figure 49* on page 99).

The steps to configure outbound rules are described in the following sections:

- *Set LAN WAN Rules*.
- *Set DMZ WAN Rules*.
- *Set LAN DMZ Rules*.

Table 18. Outbound rules overview

Setting	Description
Service	The service or application to be covered by this rule. If the service or application does not appear in the list, you need to define it using the Services screen (see *Add Customized Services* on page 112).
Action	The action for outgoing connections covered by this rule: • **BLOCK always** • **BLOCK by schedule, otherwise allow** • **ALLOW always** • **ALLOW by schedule, otherwise block** **Note:** Any outbound traffic that is not blocked by rules you create is allowed by the default rule. **Note:** ALLOW rules are useful only if the traffic is already covered by a BLOCK rule. That is, you wish to allow a subset of traffic that is currently blocked by another rule.
Select Schedule	The time schedule (that is, Schedule1, Schedule2, or Schedule3) that is used by this rule. • This drop-down list is activated only when BLOCK by schedule, otherwise allow or ALLOW by schedule, otherwise block is selected as the Action. • Use the schedule screen to configure the time schedules (see *Set a Schedule to Block or Allow Specific Traffic* on page 121).

Table 18. Outbound rules overview (continued)

Setting	Description
LAN Users	The settings that determine which computers on your network are affected by this rule. The options are: • **Any**. All PCs and devices on your LAN. • **Single address**. Enter the required address to apply the rule to a single device on your LAN. • **Address range**. Enter the required addresses in the Start and End fields to apply the rule to a range of devices. • **Groups**. Select the group to which the rule applies. Use the LAN Groups screen to assign PCs to groups. See *Manage Groups and Hosts (LAN Groups)* on page 67. • **IP Group**. Select the IP group to which the rule applies. Use the IP Groups screen to assign IP addresses to groups. See *Create IP Groups* on page 114.
WAN Users	The settings that determine which Internet locations are covered by the rule, based on their IP address. The options are: • **Any**. All Internet IP address are covered by this rule. • **Single address**. Enter the required address in the Start field. • **Address range**. Fill in the Start and End fields. • **IP Group**. Select the IP group to which the rule applies. Use the IP Groups screen to assign IP addresses to groups. See *Create IP Groups* on page 114.
DMZ Users	The settings that determine which DMZ computers on the DMZ network are affected by this rule. The options are: • **Any**. All PCs and devices on your DMZ network. • **Single address**. Enter the required address to apply the rule to a single PC on the DMZ network. • **Address range**. Enter the required addresses in the Start and End fields to apply the rule to a range of DMZ computers.
QoS Profile	The priority assigned to IP packets of this service. The priorities are defined by the *Type of Service (ToS) in the Internet Protocol Suite standards*, RFC 1349. The QoS profile determines the priority of a service, which, in turn, determines the quality of that service for the traffic passing through the firewall. The VPN firewall marks the Type of Service (ToS) field as defined in the QoS profiles that you create. For more information, see *Create Quality of Service (QoS) Profiles* on page 116. **Note:** There is no default QoS profile on the VPN firewall. After you have created a QoS profile, it can become active only when you apply it to a non-blocking inbound or outbound firewall rule. **Note:** This field is not applicable to LAN DMZ rules.

Table 18. Outbound rules overview (continued)

Setting	Description
Bandwidth Profile	Bandwidth limiting determines the way in which the data is sent to and from your host. The purpose of bandwidth limiting is to provide a solution for limiting the outgoing and incoming traffic, thus preventing the LAN users from consuming all the bandwidth of the Internet link. For more information, see *Create Bandwidth Profiles* on page 118. Bandwidth limiting occurs in the following ways: • For outbound traffic. On the available WAN interface in the single WAN port mode and auto-rollover mode, and on the selected interface in load balancing mode. • For inbound traffic. On the LAN interface for all WAN modes. **Note:** Bandwidth limiting does not apply to the DMZ interface.
Log	The setting that determines whether packets covered by this rule are logged. The options are: • **Always**. Always log traffic considered by this rule, whether it matches or not. This is useful when you are debugging your rules. • **Never**. Never log traffic considered by this rule, whether it matches or not.
NAT IP	The setting that specifies whether the source address of the outgoing packets on the WAN should be auto-detected, should be assigned the address of a WAN interface, or should be assigned the address of a different interface. The options are: • **Auto**. The source address of the outgoing packets is auto-detected via the configured routing and load balancing rules. • **WAN Interface Address**. All the outgoing packets on the WAN are assigned to the address of the specified WAN interface. • **Single Address**. All the outgoing packets on the WAN are assigned to the specified IP address, for example, a secondary WAN address that you have configured. **Note:** The NAT IP option is available only when the WAN mode is NAT. The IP address specified should fall under the WAN subnet.

Inbound Rules (Port Forwarding)

If you have enabled Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly access any of your local computers. However, by defining an inbound rule you can make a local server (for example, a web server or game server) visible and available to the Internet. The rule informs the firewall to direct inbound traffic for a particular service to one local server based on the destination port number. This process is also known as port forwarding.

Whether or not DHCP is enabled, how a PC accesses the server's LAN address impacts the inbound rules. For example:

- If your external IP address is assigned dynamically by your ISP (DHCP enabled), the IP address might change periodically as the DHCP lease expires. Consider using Dyamic DNS so that external users can always find your network (see *Configure Dynamic DNS* on page 42).
- If the IP address of the local server PC is assigned by DHCP, it might change when the PC is rebooted. To avoid this, use the Reserved (DHCP Client) feature in the LAN Groups

screen to keep the PC's IP address constant (see *Set Up Address Reservation* on page 72).

- Local PCs need to access the local server using the PCs' local LAN address. Attempts by local PCs to access the server using the external WAN IP address will fail.

Note: See *Configure Port Triggering* on page 130 for yet another way to allow certain types of inbound traffic that would otherwise be blocked by the firewall.

Note: The VPN firewall always blocks denial of service (DoS) attacks. A DoS attack does not attempt to steal data or damage your PCs, but overloads your Internet connection so you cannot use it (that is, the service becomes unavailable).

Note: When the Block TCP Flood and Block UDP Flood check boxes are selected on the Attack Checks screen (see *Attack Checks* on page 106), multiple concurrent connections of the same application from one host or IP address (such as multiple DNS queries from one PC) trigger the VPN firewall's DoS protection.

The following table describes the fields that define the rules for inbound traffic and that are common to most Inbound Service screens (see *Figure 44* on page 94, *Figure 47* on page 97, and *Figure 50* on page 100).

The steps to configure inbound rules are described in the following sections:

- *Set LAN WAN Rules*
- *Set DMZ WAN Rules*
- *Set LAN DMZ Rules*

Table 19. Inbound rules overview

Setting	Description
Service	The service or application to be covered by this rule. If the service or application does not appear in the list, you need to define it using the Services screen (see *Add Customized Services* on page 112).
Action	The action for outgoing connections covered by this rule: • **BLOCK always** • **BLOCK by schedule, otherwise allow** • **ALLOW always** • **ALLOW by schedule, otherwise block** **Note:** Any inbound traffic that is not blocked by rules you create is allowed by the default rule.
Select Schedule	The time schedule (that is, Schedule1, Schedule2, or Schedule3) that is used by this rule. • This drop-down list is activated only when BLOCK by schedule, otherwise allow or ALLOW by schedule, otherwise block is selected as the Action. • Use the schedule screen to configure the time schedules (see *Set a Schedule to Block or Allow Specific Traffic* on page 121).
Send to LAN Server	The LAN server address determines which computer on your network is hosting this service rule. (You can also translate this address to a port number.) The options are: • **Single address**. Enter the required address in the Start field to apply the rule to a single device on your LAN. • **Address range**. Enter the required addresses in the Start and End fields to apply the rule to a range of devices.
Send to DMZ Server	The DMZ server address determines which computer on your network is hosting this service rule. (You can also translate this address to a port number.)
Translate to Port Number	You can enable this setting and specify a port number if you want to assign the LAN server or DMZ server to a specific port.
WAN Destination IP Address	The setting that determines the destination IP address applicable to incoming traffic. This is the public IP address that maps to the internal LAN server. This address can be either the address of one of the WAN interfaces or another public IP address (when you have a secondary WAN address configured). You also have the option to enter an address range. Enter the required addresses in the Start and End fields to apply the rule to a range of devices.

Table 19. Inbound rules overview (continued)

Setting	Description
LAN Users	The settings that determine which computers on your network are affected by this rule. The options are: • **Any**. All PCs and devices on your LAN. • **Single address**. Enter the required address to apply the rule to a single device on your LAN. • **Address range**. Enter the required addresses in the Start and End fields to apply the rule to a range of devices. • **Groups**. Select the group to which the rule applies. Use the LAN Groups screen to assign PCs to groups. See *Manage Groups and Hosts (LAN Groups)* on page 67. • **IP Group**. Select the IP group to which the rule applies. Use the IP Groups screen to assign IP addresses to groups. See *Create IP Groups* on page 114. **Note:** For LAN WAN inbound rules, this field is not applicable when the WAN mode is NAT because your network presents only *one* IP address to the Internet.
WAN Users	The settings that determine which Internet locations are covered by the rule, based on their IP address. The options are: • **Any**. All Internet IP address are covered by this rule. • **Single address**. Enter the required address in the Start field. • **Address range**. Fill in the Start and End fields. • **IP Group**. Select the IP group to which the rule applies. Use the IP Groups screen to assign IP addresses to groups. See *Create IP Groups* on page 114.
DMZ Users	The settings that determine which DMZ computers on the DMZ network are affected by this rule. The options are: • **Any**. All PCs and devices on your DMZ network. • **Single address**. Enter the required address to apply the rule to a single PC on the DMZ network. • **Address range**. Enter the required addresses in the Start and End fields to apply the rule to a range of DMZ computers. **Note:** For DMZ WAN inbound rules, this field is not applicable when the WAN mode is NAT because your network presents only *one* IP address to the Internet.
QoS Profile	The priority assigned to IP packets of this service. The priorities are defined by the *Type of Service (ToS) in the Internet Protocol Suite standards*, RFC 1349. The QoS profile determines the priority of a service, which, in turn, determines the quality of that service for the traffic passing through the firewall. The VPN firewall marks the Type of Service (ToS) field as defined in the QoS profiles that you create. For more information, see *Create Quality of Service (QoS) Profiles* on page 116. **Note:** There is no default QoS profile on the VPN firewall. After you have created a QoS profile, it can become active only when you apply it to a non-blocking inbound or outbound firewall rule. **Note:** This field is not applicable to LAN DMZ rules.

Table 19. Inbound rules overview (continued)

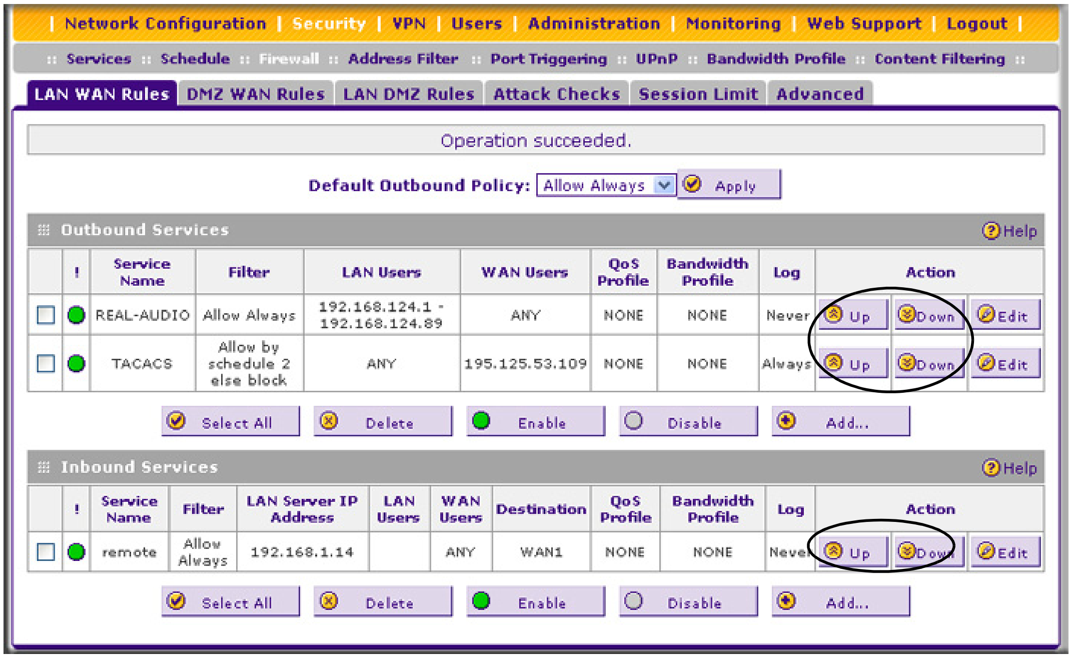
Setting	Description
Log	The setting that determines whether packets covered by this rule are logged. The options are: • **Always**. Always log traffic considered by this rule, whether it matches or not. This is useful when you are debugging your rules. • **Never**. Never log traffic considered by this rule, whether it matches or not.
Bandwidth Profile	Bandwidth limiting determines the way in which the data is sent to and from your host. The purpose of bandwidth limiting is to provide a solution for limiting the outgoing and incoming traffic, thus preventing the LAN users from consuming all the bandwidth of the Internet link. For more information, see *Create Bandwidth Profiles* on page 118. Bandwidth limiting occurs in the following ways: • For outbound traffic. On the available WAN interface in the single WAN port mode and auto-rollover mode, and on the selected interface in load balancing mode. • For inbound traffic. On the LAN interface for all WAN modes. **Note:** Bandwidth limiting does not apply to the DMZ interface.

Note: Some residential broadband ISP accounts do not allow you to run any server processes (such as a web or FTP server) from your location. Your ISP might periodically check for servers and might suspend your account if it discovers any active servers at your location. If you are unsure, see the Acceptable Use Policy of your ISP.

Order of Precedence for Rules

As you define a new rule, it is added to a table in a Rules screen as the last item in the list, as shown in the LAN WAN Rules screen example in *Figure 41* on page 91.

For any traffic attempting to pass through the firewall, the packet information is subjected to the rules in the order shown in the Rules table, beginning at the top and proceeding to the bottom. In some cases, the order of precedence of two or more rules might be important in determining the disposition of a packet. For example, you should place the most strict rules at the top (those with the most specific services or addresses). The **Up** and **Down** table buttons in the Action column allow you to relocate a defined rule to a new position in the table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced
Apply
Help
Select All
Delete
Enable
Disable
Add...

Operation succeeded.

Default Outbound Policy: Allow Always

Outbound Services

	!	Service Name	Filter	LAN Users	WAN Users	QoS Profile	Bandwidth Profile	Log	Action
□	●	REAL-AUDIO	Allow Always	192.168.124.1 - 192.168.124.89	ANY	NONE	NONE	Never	Up Down Edit
□	●	TACACS	Allow by schedule 2 else block	ANY	195.125.53.109	NONE	NONE	Always	Up Down Edit

Inbound Services

	!	Service Name	Filter	LAN Server IP Address	LAN Users	WAN Users	Destination	QoS Profile	Bandwidth Profile	Log	Action
□	●	remote	Allow Always	192.168.1.14		ANY	WAN1	NONE	NONE	Never	Up Down Edit

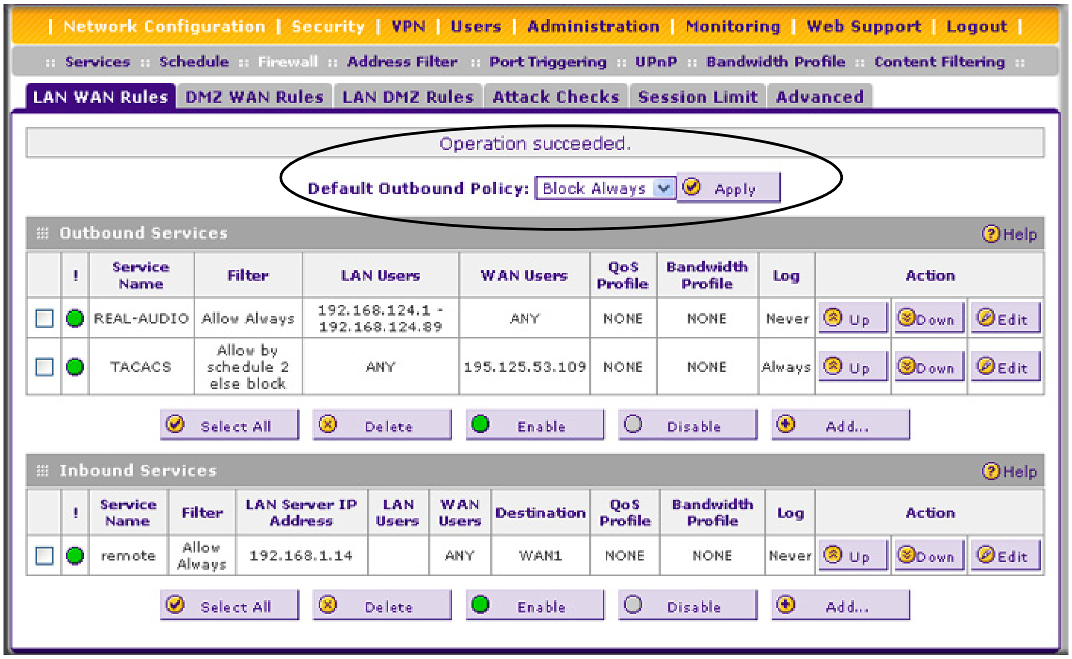
Figure 41.

Set LAN WAN Rules

The default outbound policy is to allow all traffic to the Internet to pass through. Firewall rules can then be applied to block specific types of traffic from going out from the LAN to the Internet (outbound). This feature is also referred to as service blocking. You can change the default policy of Allow Always to Block Always to block all outbound traffic, which then allows you to enable only specific services to pass through the VPN firewall.

➢ To change the default outbound policy:

1. Select **Security > Firewall**. The Firewall submenu tabs display, with the LAN WAN Rules screen in view. (The following figure shows some examples.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced
Apply
Help
Select All
Delete
Enable
Disable
Add...

Operation succeeded.

Default Outbound Policy: Block Always

Outbound Services

	!	Service Name	Filter	LAN Users	WAN Users	QoS Profile	Bandwidth Profile	Log	Action		
□	●	REAL-AUDIO	Allow Always	192.168.124.1 - 192.168.124.89	ANY	NONE	NONE	Never	Up	Down	Edit
□	●	TACACS	Allow by schedule 2 else block	ANY	195.125.53.109	NONE	NONE	Always	Up	Down	Edit

Inbound Services

	!	Service Name	Filter	LAN Server IP Address	LAN Users	WAN Users	Destination	QoS Profile	Bandwidth Profile	Log	Action		
□	●	remote	Allow Always	192.168.1.14		ANY	WAN1	NONE	NONE	Never	Up	Down	Edit

Figure 42.

2. Next to Default Outbound Policy, select **Block Always** from the drop-down list.
3. Next to the drop-down list, click the **Apply** table button.

➢ To make changes to an existing outbound or inbound service rule:

In the Action column to the right of the rule, click one of the following table buttons:

- **Edit**. Allows you to make any changes to the definition of an existing rule. Depending on your selection, either the Edit LAN WAN Outbound Service screen (identical to *Figure 43* on page 93) or Edit LAN WAN Inbound Service screen (identical to *Figure 44* on page 94) displays, containing the data for the selected rule.
- **Up**. Moves the rule up one position in the table rank.
- **Down**. Moves the rule down one position in the table rank.

➢ To enable, disable, or delete one or more rules:

1. Select the check box to the left of the rule that you want to enable, disable, or delete, or click the **Select All** table button to select all rules.
2. Click one of the following table buttons:
   - **Enable**. Enables the rule or rules. The “!” status icon changes from a gray circle to a green circle, indicating that the selected rule or rules are enabled. (By default, when a rule is added to the table, it is automatically enabled.)
   - **Disable**. Disables the rule or rules. The “!” status icon changes from a green circle to a gray circle, indicating that the selected rule or rules are disabled.
   - **Delete**. Deletes the rule or rules.

LAN WAN Outbound Services Rules

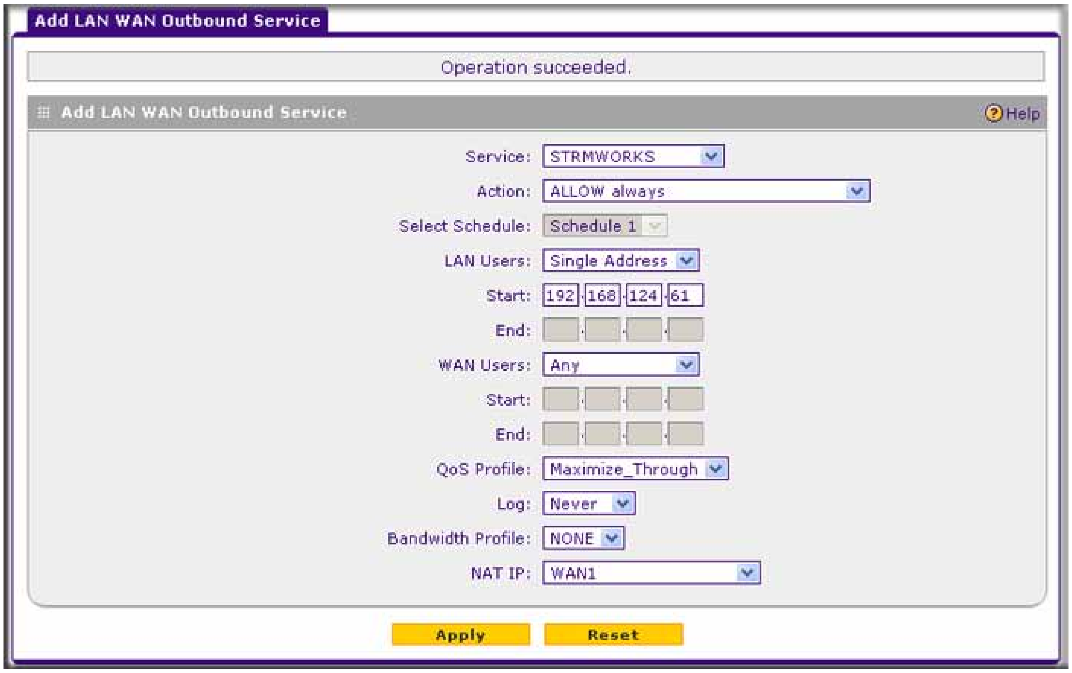
You can define rules that specify exceptions to the default rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. An outbound rule can block or allow traffic between an internal IP LAN address and any external WAN IP address according to the schedule created in the Schedule screen.

You can also tailor these rules to your specific needs (see *Administrator Tips* on page 82).

> **Note:** This feature is for advanced administrators only! Incorrect configuration might cause serious problems.

➤ **To create a new outbound LAN WAN service rule:**

1. In the LAN WAN Rules screen, click the **Add** table button under the Outbound Services table. The Add LAN WAN Outbound Service screen displays. (The following figure shows an example.)



Add LAN WAN Outbound Service

Operation succeeded.

Add LAN WAN Outbound Service

Service:	STRMWORKS
Action:	ALLOW always
Select Schedule:	Schedule 1
LAN Users:	Single Address
Start:	192.168.124.61
End:	
WAN Users:	Any
Start:	
End:	
QoS Profile:	Maximize_Through
Log:	Never
Bandwidth Profile:	NONE
NAT IP:	WAN1

Figure 43.

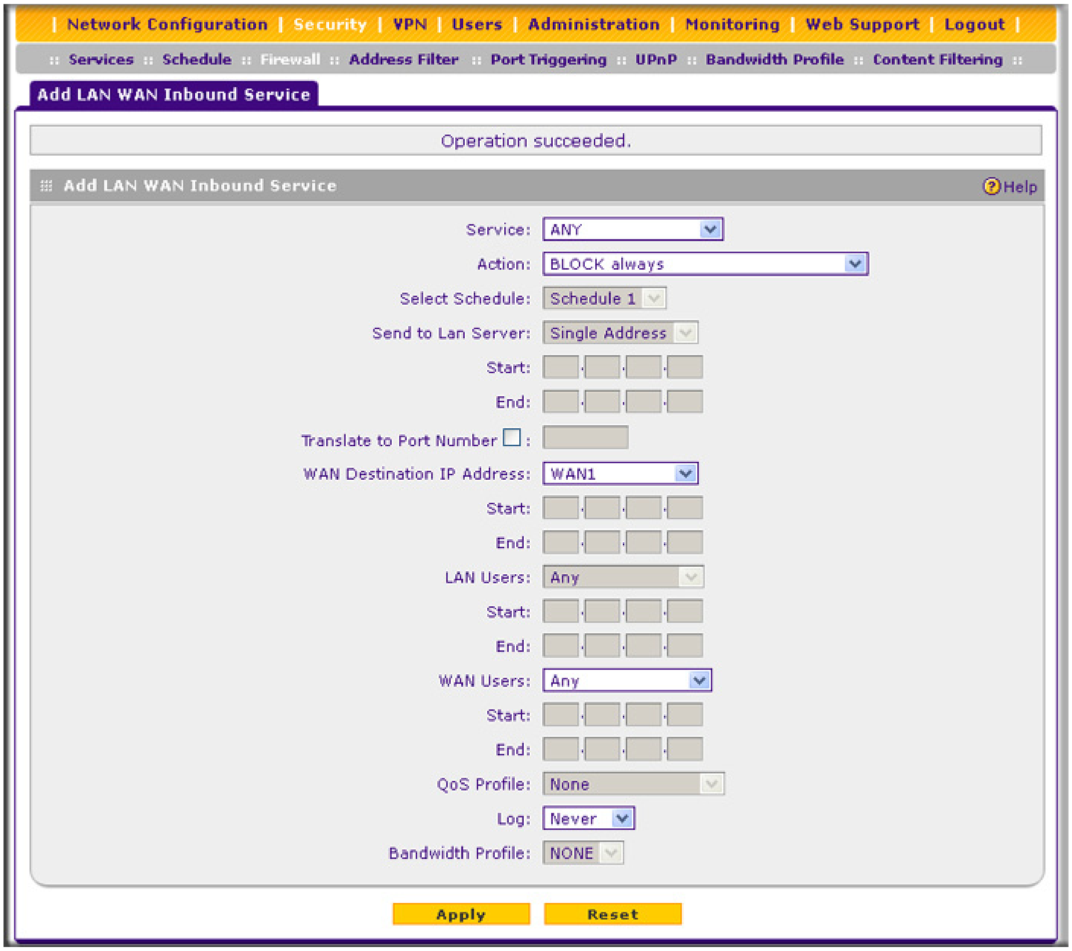
2. Enter the settings as explained in *Table 18* on page 84.
3. Click **Apply** to save your changes. The new rule is now added to the Outbound Services table.

LAN WAN Inbound Services Rules

The Inbound Services table lists all existing rules for inbound traffic. If you have not defined any rules, no rules are listed. By default, all inbound traffic (from the Internet to the LAN) is blocked. Remember that allowing inbound services opens potential security holes in your firewall. Enable only those ports that are necessary for your network.

➤ **To create a new inbound LAN WAN service rule:**

1. In the LAN WAN Rules screen, click the **Add** table button under the Inbound Services table. The Add LAN WAN Inbound Service screen displays. (The following figure shows an example.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Add LAN WAN Inbound Service
Help
Apply
Reset

Operation succeeded.

Add LAN WAN Inbound Service

Service:	ANY
Action:	BLOCK always
Select Schedule:	Schedule 1
Send to Lan Server:	Single Address
Start:	
End:	
Translate to Port Number □ :	
WAN Destination IP Address:	WAN1
Start:	
End:	
LAN Users:	Any
Start:	
End:	
WAN Users:	Any
Start:	
End:	
QoS Profile:	None
Log:	Never
Bandwidth Profile:	NONE

Figure 44.

2. Enter the settings as explained in *Table 19* on page 88.

3. Click **Apply** to save your changes. The new rule is now added to the Inbound Services table.

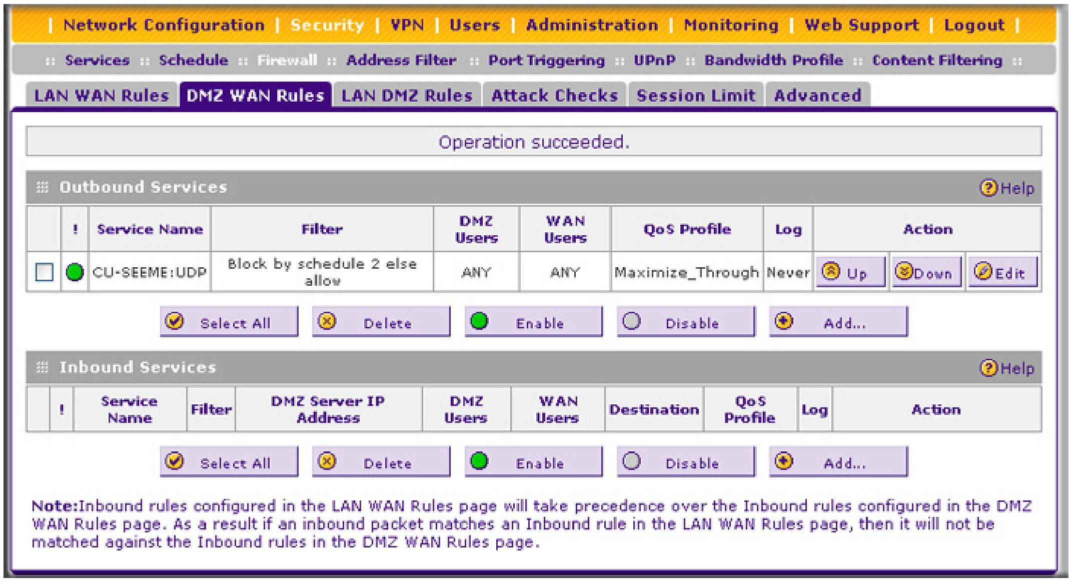
Set DMZ WAN Rules

The firewall rules for traffic between the DMZ and the Internet are configured on the DMZ WAN Rules screen. The default outbound policy is to allow all traffic from and to the Internet to pass through. You can then apply firewall rules to block specific types of traffic from either going out from the DMZ to the Internet (outbound) or coming in from the Internet to the DMZ (inbound).

There is no drop-down list that lets you set the default outbound policy as there is on the LAN WAN Rules screen. You can change the default outbound policy by blocking all outbound traffic and then enabling only specific services to pass through the VPN firewall. You do so by adding outbound services rules (see *DMZ WAN Outbound Services Rules* on page 96).

➢ To access the DMZ WAN Rules screen:

1. Select **Security > Firewall > DMZ WAN Rules**. The DMZ WAN Rules screen displays. (The following figure shows a rule in the Outbound Services table as an example.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced

Operation succeeded.

Outbound Services

	!	Service Name	Filter	DMZ Users	WAN Users	QoS Profile	Log	Action
□	●	CU-SEEME:UDP	Block by schedule 2 else allow	ANY	ANY	Maximize_Through	Never	Up Down Edit

Select All
Delete
Enable
Disable
Add...

Inbound Services

	!	Service Name	Filter	DMZ Server IP Address	DMZ Users	WAN Users	Destination	QoS Profile	Log	Action

Select All
Delete
Enable
Disable
Add...

Note: Inbound rules configured in the LAN WAN Rules page will take precedence over the Inbound rules configured in the DMZ WAN Rules page. As a result if an inbound packet matches an Inbound rule in the LAN WAN Rules page, then it will not be matched against the Inbound rules in the DMZ WAN Rules page.

Figure 45.

➢ To make changes to an existing outbound or inbound service rule:

In the Action column to the right of the rule, click one of the following table buttons:

- **Edit**. Allows you to make any changes to the rule definition of an existing rule. Depending on your selection, either the Edit DMZ WAN Outbound Service screen (identical to *Figure 46* on page 96) or the Edit DMZ WAN Inbound Service screen (identical to *Figure 47* on page 97) displays, containing the data for the selected rule.
- **Up**. Moves the rule up one position in the table rank.
- **Down**. Moves the rule down one position in the table rank.

➤ **To delete or disable one or more rules:**

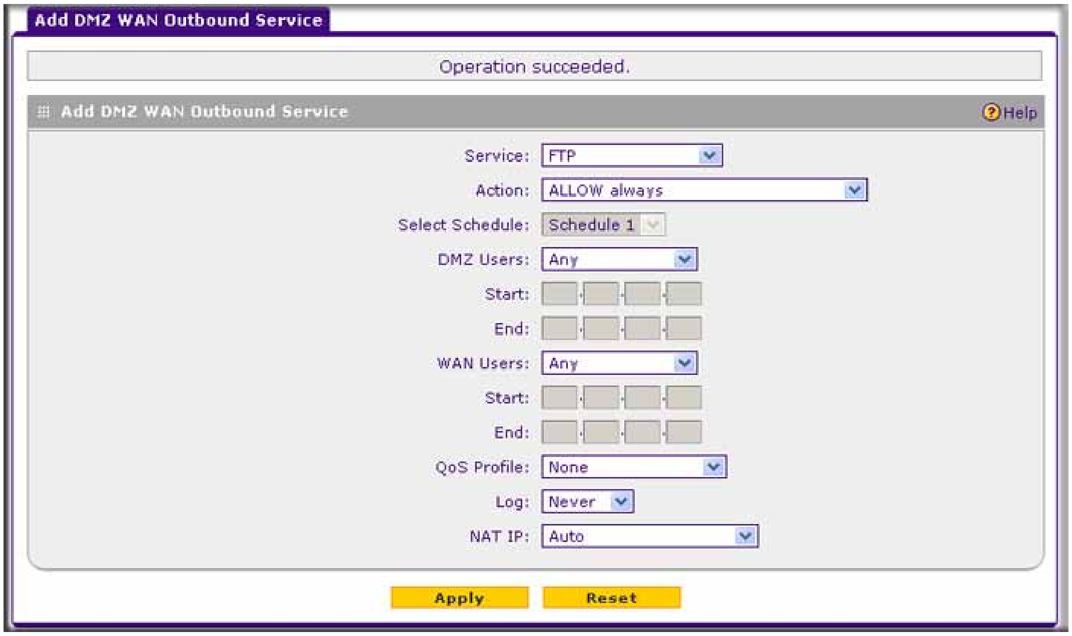
1. Select the check box to the left of the rule that you want to delete or disable, or click the **Select All** table button to select all rules.
2. Click one of the following table buttons:
   - **Disable**. Disables the rule or rules. The “!” status icon changes from a green circle to a gray circle, indicating that the selected rule or rules are disabled. (By default, when a rule is added to the table, it is automatically enabled.)
   - **Delete**. Deletes the selected rule or rules.

DMZ WAN Outbound Services Rules

You can change the default outbound policy or define rules that specify exceptions to the default outbound policy. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. An outbound rule can block or allow traffic between the DMZ and any external WAN IP address according to the schedule created in the Schedule screen.

➤ **To create a new outbound DMZ WAN service rule:**

1. In the DMZ WAN Rules screen, click the **Add** table button under the Outbound Services table. The Add DMZ WAN Outbound Service screen displays. (The following figure shows an example.)



Add DMZ WAN Outbound Service

Operation succeeded.

Add DMZ WAN Outbound Service

Service:	FTP
Action:	ALLOW always
Select Schedule:	Schedule 1
DMZ Users:	Any
Start:	
End:	
WAN Users:	Any
Start:	
End:	
QoS Profile:	None
Log:	Never
NAT IP:	Auto

Figure 46.

2. Enter the settings as explained in *Table 18* on page 84.
3. Click **Apply.** The new rule is now added to the Outbound Services table. The rule is automatically enabled.

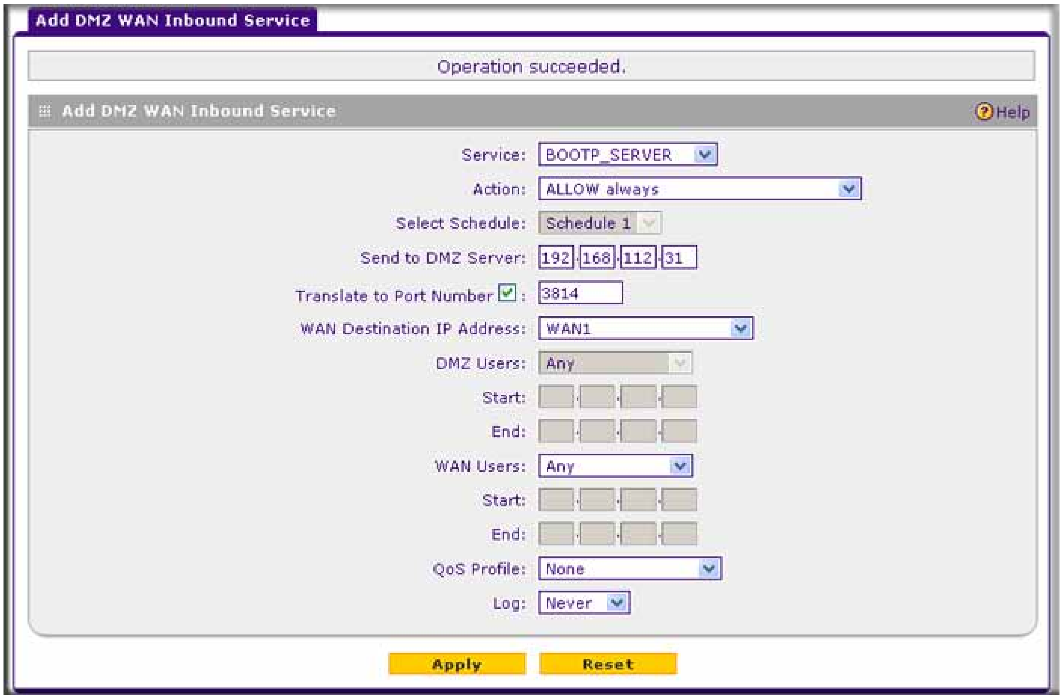
DMZ WAN Inbound Services Rules

The Inbound Services table lists all existing rules for inbound traffic. If you have not defined any rules, no rules are listed. By default, all inbound traffic (from the Internet to the DMZ) is allowed.

Inbound rules that are configured on the LAN WAN Rules screen take precedence over inbound rules that are configured on the DMZ WAN Rules screen. As a result, if an inbound packet matches an inbound rule on the LAN WAN Rules screen, it is not matched against the inbound rules on the DMZ WAN Rules screen.

➤ **To create a new inbound DMZ WAN service rule:**

1. In the DMZ WAN Rules screen, click the **Add** table button under the Inbound Services table. The Add DMZ WAN Inbound Service screen displays. (The following figure shows an example.)



Add DMZ WAN Inbound Service

Operation succeeded.

Add DMZ WAN Inbound Service

Service:	BOOTP_SERVER
Action:	ALLOW always
Select Schedule:	Schedule 1
Send to DMZ Server:	192.168.112.31
Translate to Port Number ☑:	3814
WAN Destination IP Address:	WAN1
DMZ Users:	Any
Start:	. . .
End:	. . .
WAN Users:	Any
Start:	. . .
End:	. . .
QoS Profile:	None
Log:	Never

Figure 47.

2. Enter the settings as explained in *Table 19* on page 88.
3. Click **Apply** to save your changes. The new rule is now added to the Inbound Services table.

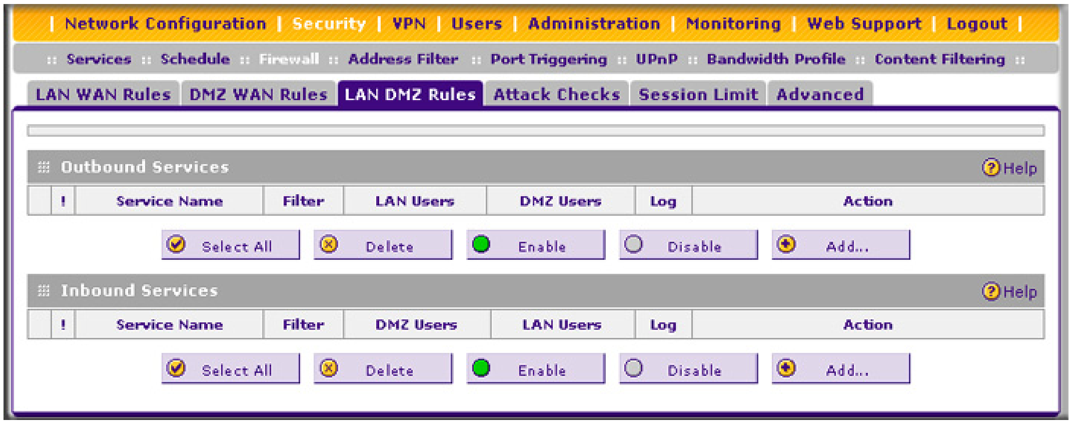
Set LAN DMZ Rules

The LAN DMZ Rules screen allows you to create rules that define the movement of traffic between the LAN and the DMZ. The default outbound and inbound policies are to allow all traffic between the local LAN and DMZ network. You can then apply firewall rules to block specific types of traffic from either going out from the LAN to the DMZ (outbound) or coming in from the DMZ to the LAN (inbound).

There is no drop-down list that lets you set the default outbound policy as there is on the LAN WAN Rules screen. You can change the default outbound policy by blocking all outbound traffic and then enabling only specific services to pass through the VPN firewall. You do so by adding outbound services rules (see *LAN DMZ Outbound Services Rules* on page 99).

➢ To access the LAN DMZ Rules screen:

1. Select **Security > Firewall > LAN DMZ Rules**. The LAN DMZ Rules screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced
Outbound Services
Help
Select All
Delete
Enable
Disable
Add...
Inbound Services
Help
Select All
Delete
Enable
Disable
Add...

Outbound Services

	!	Service Name	Filter	LAN Users	DMZ Users	Log	Action

Inbound Services

	!	Service Name	Filter	DMZ Users	LAN Users	Log	Action

Figure 48.

➢ To make changes to an existing outbound or inbound service rule:

In the Action column to the right of the rule, click one of the following table buttons:

- **Edit**. Allows you to make any changes to the rule definition of an existing rule. Depending on your selection, either the Edit LAN DMZ Outbound Service screen (identical to *Figure 49* on page 99) or Edit LAN DMZ Inbound Service screen (identical to *Figure 50* on page 100) displays, containing the data for the selected rule.
- **Up**. Moves the rule up one position in the table rank.
- **Down**. Moves the rule down one position in the table rank.

➤ To delete or disable one or more rules:

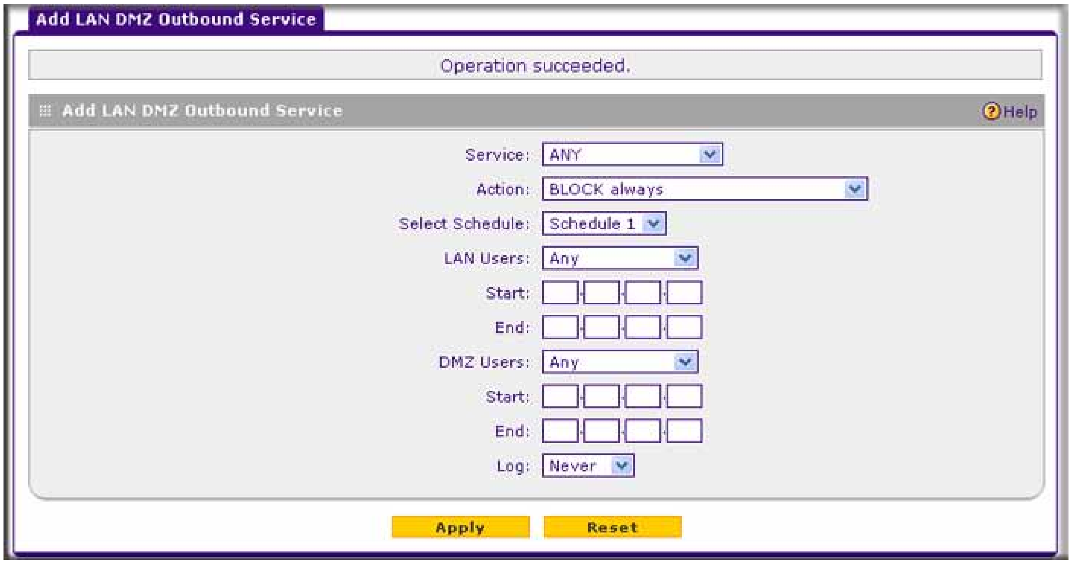
1. Select the check box to the left of the rule that you want to delete or disable, or click the **Select All** table button to select all rules.
2. Click one of the following table buttons:
   - **Disable**. Disables the rule or rules. The “!” status icon changes from a green circle to a gray circle, indicating that the selected rule or rules are disabled. (By default, when a rule is added to the table, it is automatically enabled.)
   - **Delete**. Deletes the selected rule or rules.

LAN DMZ Outbound Services Rules

You can change the default outbound policy or define rules that specify exceptions to the default outbound policy. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. An outbound rule can block or allow traffic between the DMZ and any internal LAN IP address according to the schedule created in the Schedule screen.

➤ To create a new outbound LAN DMZ service rule:

1. In the LAN DMZ Rules screen, click the **Add** table button under the Outbound Services table. The Add LAN DMZ Outbound Service screen displays:



Add LAN DMZ Outbound Service

Operation succeeded.

Add LAN DMZ Outbound Service

Service:	ANY
Action:	BLOCK always
Select Schedule:	Schedule 1
LAN Users:	Any
Start:	
End:	
DMZ Users:	Any
Start:	
End:	
Log:	Never

Figure 49.

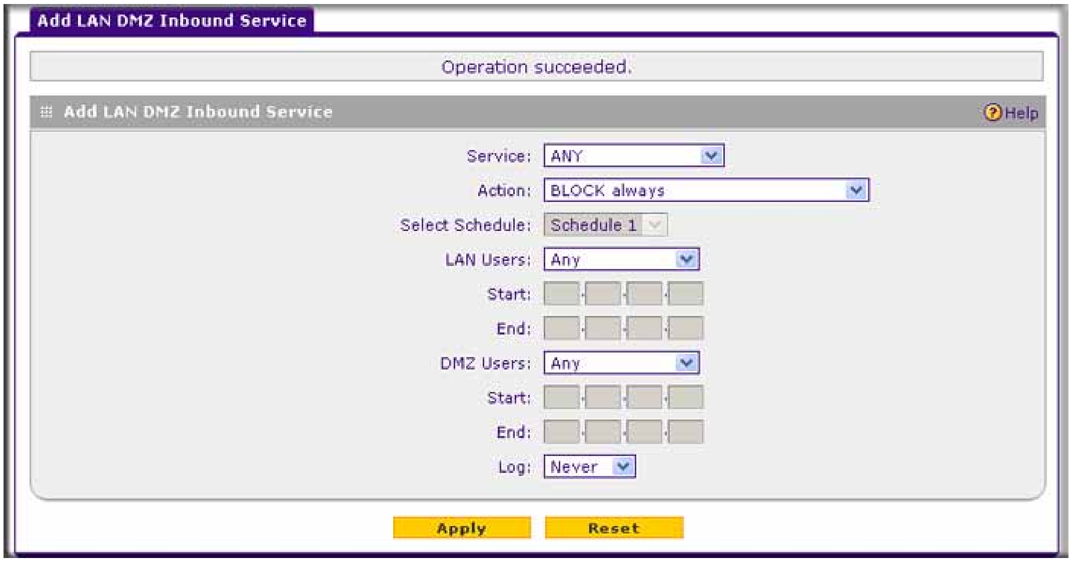
2. Enter the settings as explained in *Table 18* on page 84.
3. Click **Apply.** The new rule is now added to the Outbound Services table. The rule is automatically enabled.

LAN DMZ Inbound Services Rules

The Inbound Services table lists all existing rules for inbound traffic. If you have not defined any rules, no rules are listed. By default, all inbound traffic (from the LAN to the DMZ) is allowed.

➢ To create a new inbound LAN DMZ service rule:

1. In the LAN DMZ Rules screen, click the **Add** table button under the Inbound Services table. The Add LAN DMZ Inbound Service screen displays:



Add LAN DMZ Inbound Service

Operation succeeded.

Add LAN DMZ Inbound Service

Service:	ANY
Action:	BLOCK always
Select Schedule:	Schedule 1
LAN Users:	Any
Start:	
End:	
DMZ Users:	Any
Start:	
End:	
Log:	Never

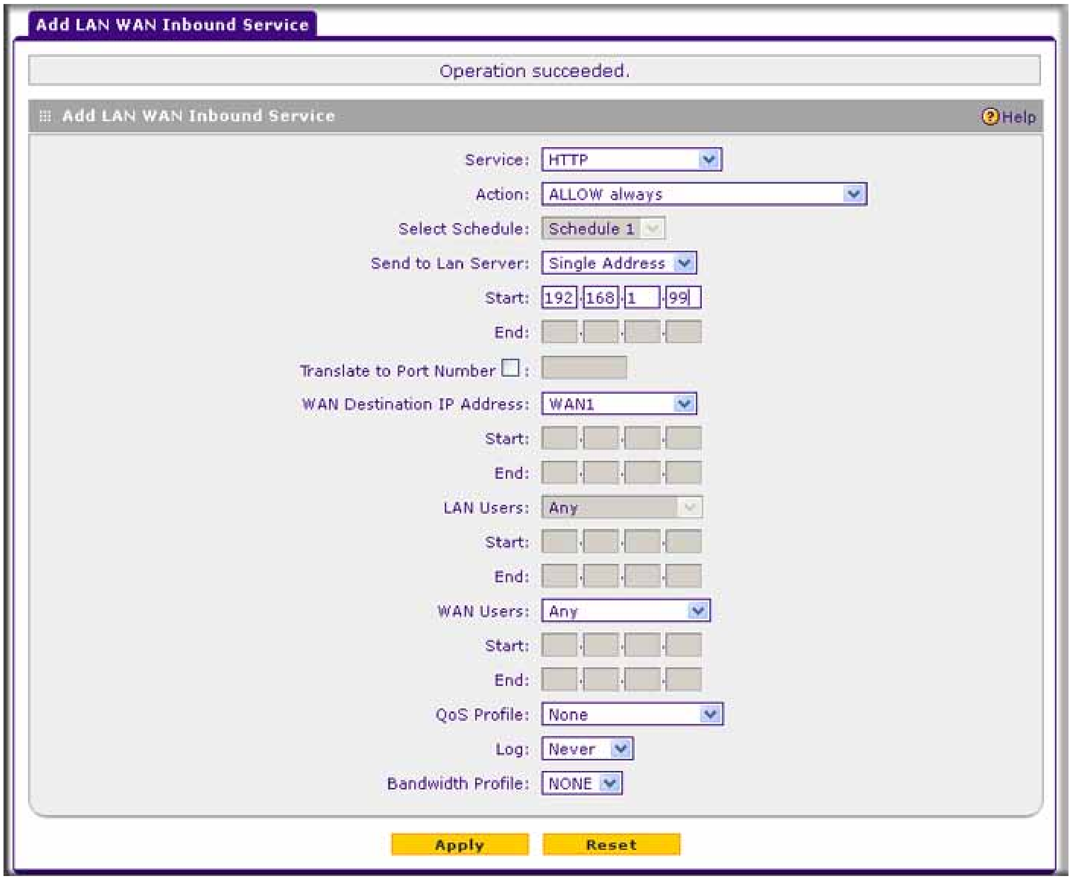
Figure 50.

2. Enter the settings as explained in *Table 19* on page 88.
3. Click **Apply** to save your changes. The new rule is now added to the Inbound Services table.

Inbound Rules Examples

LAN WAN Inbound Rule: Hosting a Local Public Web Server

If you host a public web server on your local network, you can define a rule to allow inbound web (HTTP) requests from any outside IP address to the IP address of your web server at any time of the day.



Add LAN WAN Inbound Service

Operation succeeded.

Add LAN WAN Inbound Service

Service: HTTP

Action: ALLOW always

Select Schedule: Schedule 1

Send to Lan Server: Single Address

Start: 192 . 168 . 1 . 99

End:

Translate to Port Number □ :

WAN Destination IP Address: WAN1

Start:

End:

LAN Users: Any

Start:

End:

WAN Users: Any

Start:

End:

QoS Profile: None

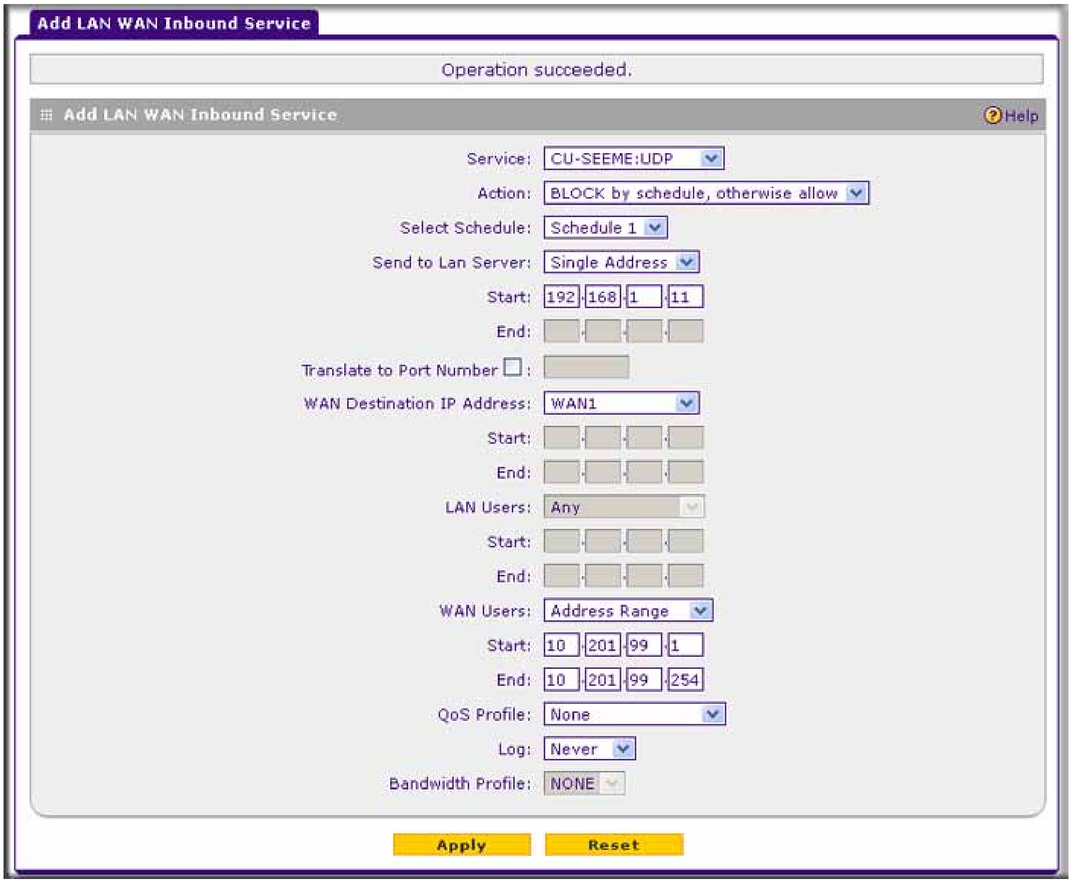
Log: Never

Bandwidth Profile: NONE

Figure 51.

LAN WAN Inbound Rule: Allowing Videoconference from Restricted Addresses

If you want to allow incoming videoconferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office, you can create an inbound rule (see the following figure). In the example, CU-SeeMe connections are allowed only from a specified range of external IP addresses.



Operation succeeded.

Add LAN WAN Inbound Service

Service:	CU-SEEME:UDP
Action:	BLOCK by schedule, otherwise allow
Select Schedule:	Schedule 1
Send to Lan Server:	Single Address
Start:	192.168.1.11
End:	
Translate to Port Number □:	
WAN Destination IP Address:	WAN1
Start:	
End:	
LAN Users:	Any
Start:	
End:	
WAN Users:	Address Range
Start:	10.201.99.1
End:	10.201.99.254
QoS Profile:	None
Log:	Never
Bandwidth Profile:	NONE

Figure 52.

LAN WAN or DMZ WAN Inbound Rule: Setting Up One-to-One NAT Mapping

In this example, we will configure multi-NAT to support multiple public IP addresses on one WAN interface. By creating an inbound rule, we will configure the VPN firewall to host an additional public IP address and associate this address with a web server on the LAN.

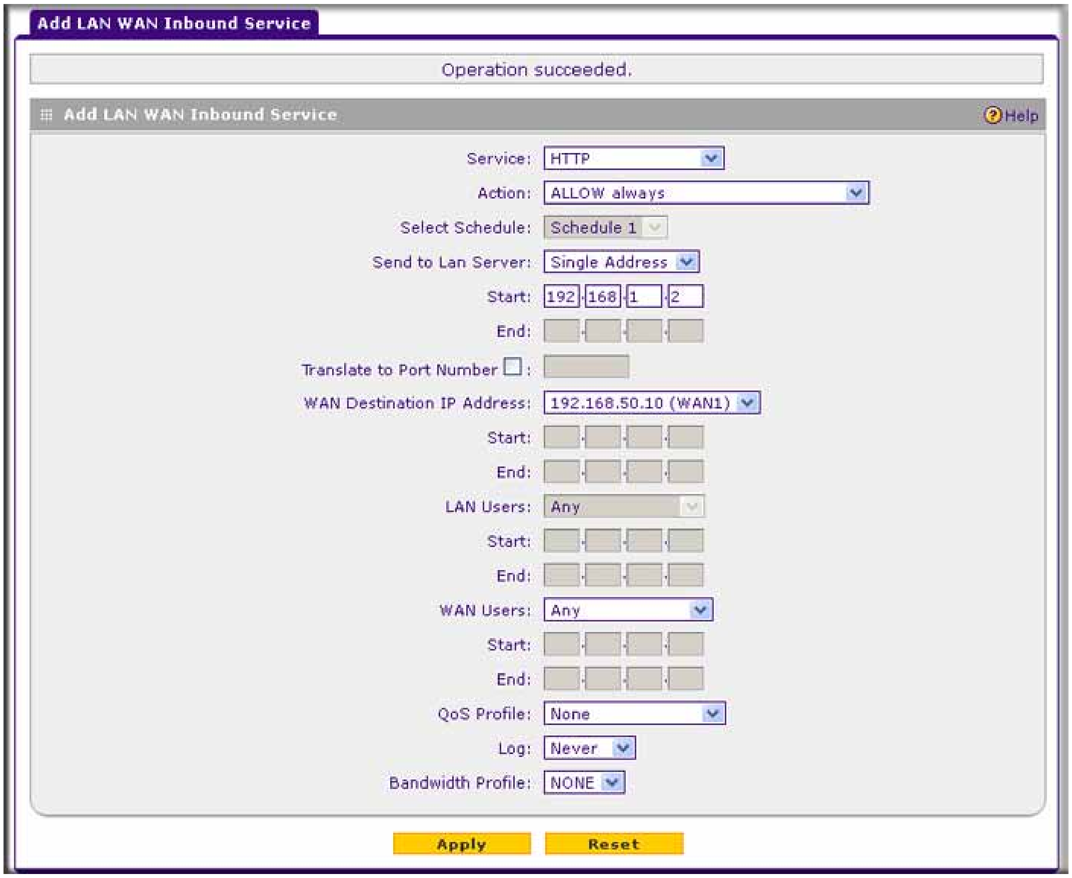
The following addressing scheme is used to illustrate this procedure:

- NETGEAR VPN firewall:
  - WAN1 IP address: 99.180.226.101
  - LAN IP address subnet: 192.168.1.1; subnet 255.255.255.0
  - DMZ IP address subnet: 192.168.10.1; subnet 255.255.255.0
- Web server PC on the VPN firewall’s LAN
  - LAN IP address: 192.168.1.2
  - DMZ IP address: 192.168.10.2
  - Access to web server is (simulated) public IP address: 192.168.55.110

Tip: If you arrange with your ISP to have more than one public IP address for your use, you can use the additional public IP addresses to map to servers on your LAN or DMZ. One of these public IP addresses is used as the primary IP address of the router that provides Internet access to your LAN PCs through NAT. The other addresses are available to map to your servers.

➤ To configure the VPN firewall for additional IP addresses:

1. Select **Security > Firewall**. The Firewall submenu tabs display.
2. If your server is to be on your LAN, select the **LAN WAN Rules** submenu tab. (This is the screen we will use in this example). If your server is to be on your DMZ, select **DMZ WAN Rules** submenu tab.
3. Click the **Add** table button under the Inbound Services table. The Add LAN WAN Inbound Service screen displays:



Operation succeeded.

Add LAN WAN Inbound Service

Service: HTTP
Action: ALLOW always
Select Schedule: Schedule 1
Send to Lan Server: Single Address
Start: 192 . 168 . 1 . 2
End:
Translate to Port Number □:
WAN Destination IP Address: 192.168.50.10 (WAN1)
Start:
End:
LAN Users: Any
Start:
End:
WAN Users: Any
Start:
End:
QoS Profile: None
Log: Never
Bandwidth Profile: NONE

Figure 53.

4. From the Service drop-down list, select **HTTP** for a web server.
5. From the Action drop-down list, select **ALLOW Always**.
6. In the Send to LAN Server field, enter the local IP address of your web server PC (192.168.1.2 in this example).
7. From the WAN Destination IP Address drop-down list, select the web server. In this example, the secondary 192.168.55.10 (WAN1) address is shown. You first need to define this address on the WAN1 Secondary Addresses screen (see *Configure Secondary WAN Addresses* on page 41) before you can select it from the WAN Destination IP Address drop-down list.
8. Click **Apply** to save your settings. The rule is now added to the Inbound Services table of the LAN WAN Rules screen.

To test the connection from a PC on the Internet, type **http://*<IP_address>***, in which <IP_address> is the public IP address that you have mapped to your web server. You should see the home page of your web server.

LAN WAN or DMZ WAN Inbound Rule: Specifying an Exposed Host

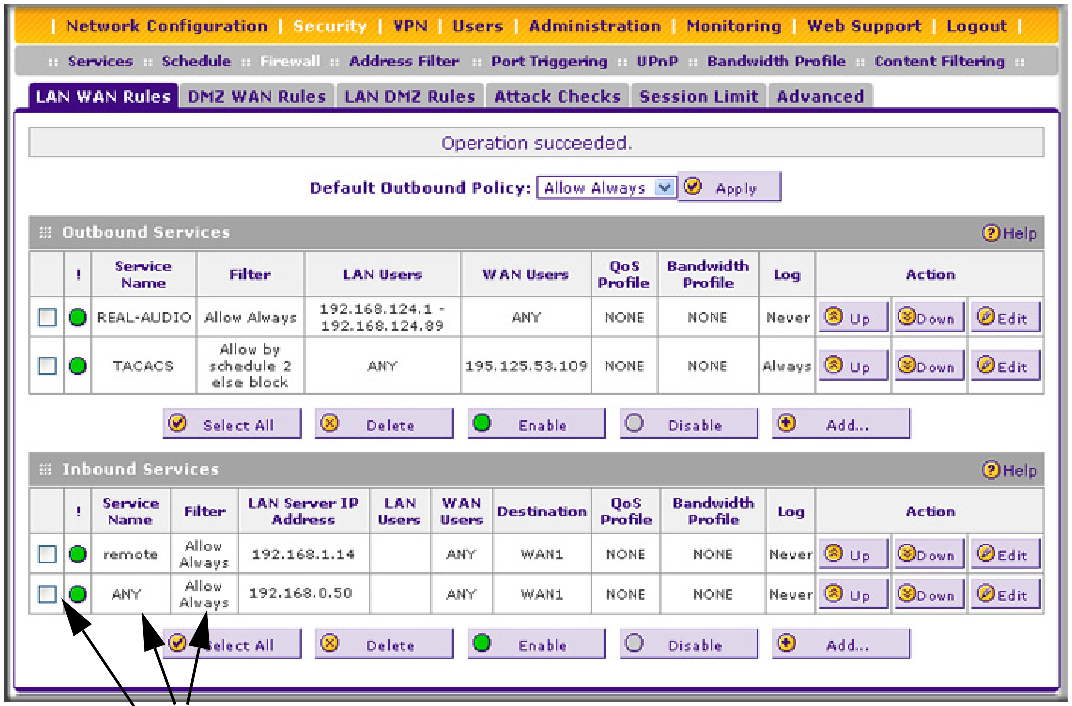
Specifying an exposed host allows you to set up a computer or server that is available to anyone on the Internet for services that you have not yet defined.

➢ **To expose one of the PCs on your LAN or DMZ as this host:**

1. Create an inbound rule that allows all protocols.
2. Place the rule below all other inbound rules. (See an example in the following figure.)

WARNING!

For security, NETGEAR strongly recommends that you avoid creating an exposed host. When a computer is designated as the exposed host, it loses much of the protection of the firewall and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced
Help
Select All
Delete
Enable
Disable
Add...

Operation succeeded.

Default Outbound Policy: Allow Always ✓ Apply

Outbound Services

	!	Service Name	Filter	LAN Users	WAN Users	QoS Profile	Bandwidth Profile	Log	Action		
□	●	REAL-AUDIO	Allow Always	192.168.124.1 - 192.168.124.89	ANY	NONE	NONE	Never	Up	Down	Edit
□	●	TACACS	Allow by schedule 2 else block	ANY	195.125.53.109	NONE	NONE	Always	Up	Down	Edit

Inbound Services

	!	Service Name	Filter	LAN Server IP Address	LAN Users	WAN Users	Destination	QoS Profile	Bandwidth Profile	Log	Action		
□	●	remote	Allow Always	192.168.1.14		ANY	WAN1	NONE	NONE	Never	Up	Down	Edit
□	●	ANY	Allow Always	192.168.0.50		ANY	WAN1	NONE	NONE	Never	Up	Down	Edit

1. Select Any and Allow Always (or Allow by Schedule).

2. Place the rule below all other inbound rules.

Figure 54.

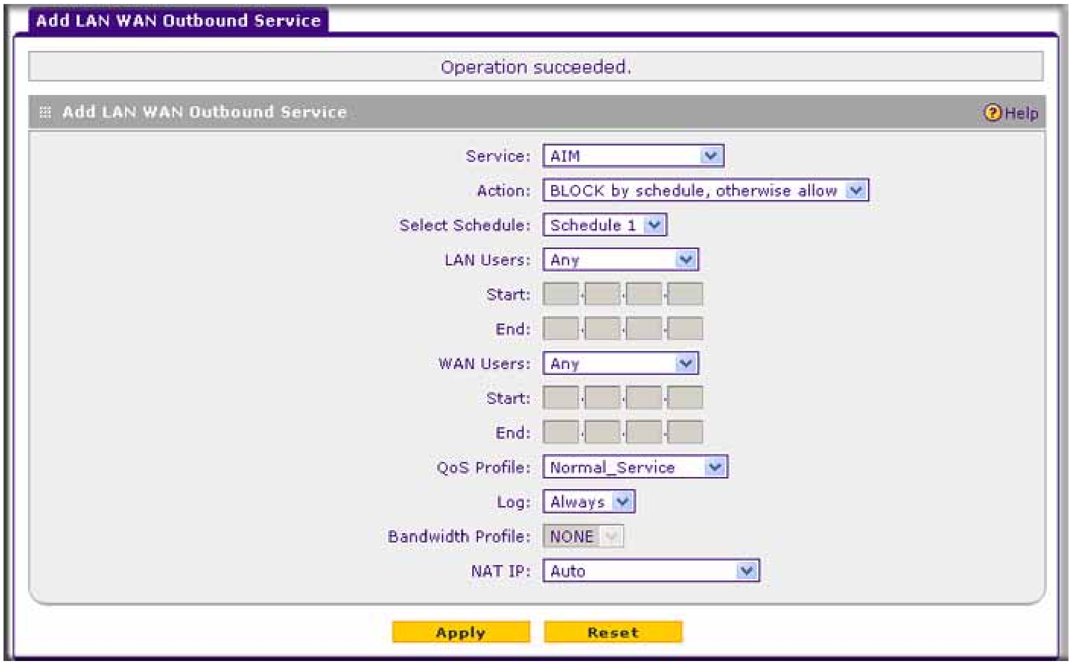
Outbound Rules Example

Outbound rules let you prevent users from using applications such as Instant Messenger, Real Audio, or other nonessential sites.

LAN WAN Outbound Rule: Blocking Instant Messenger

If you want to block Instant Messenger usage by employees during working hours, you can create an outbound rule to block that application from any internal IP address to any external address according to the schedule that you have created in the Schedule screen. (See an example in the following figure.)

You can also enable the VPN firewall to log any attempt to use Instant Messenger during the blocked period.



Add LAN WAN Outbound Service

Operation succeeded.

Add LAN WAN Outbound Service

Service:	AIM
Action:	BLOCK by schedule, otherwise allow
Select Schedule:	Schedule 1
LAN Users:	Any
Start:	
End:	
WAN Users:	Any
Start:	
End:	
QoS Profile:	Normal_Service
Log:	Always
Bandwidth Profile:	NONE
NAT IP:	Auto

Figure 55.

Configure Other Firewall Features

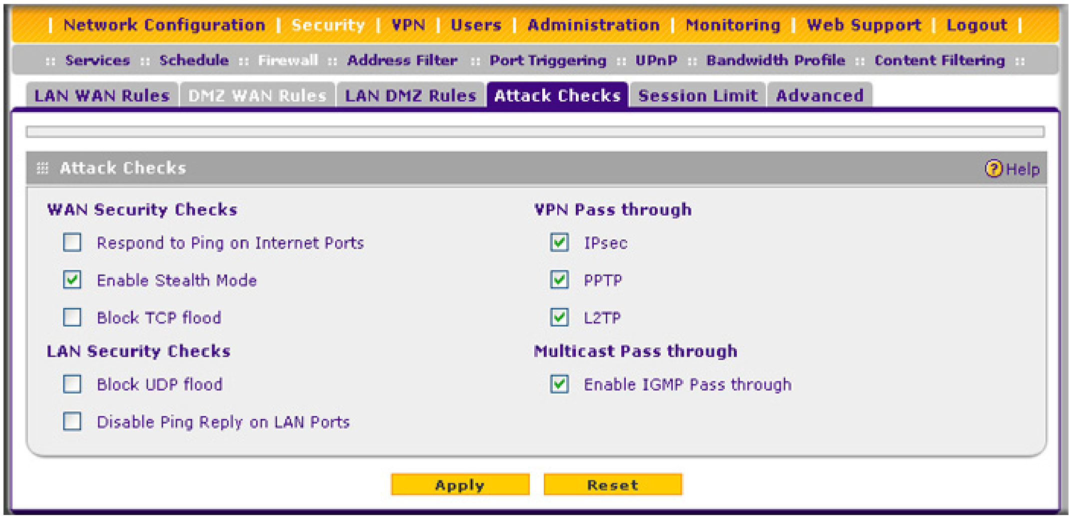
You can configure attack checks, set session limits, and manage the application level gateway (ALG) for Session Initiation Protocol (SIP) sessions.

Attack Checks

The Attack Checks screen allows you to specify whether or not the VPN firewall should be protected against common attacks in the DMZ, LAN, and WAN networks. The various types of attack checks are listed on the Attack Checks screen and defined in the following table.

➤ **To enable the appropriate attack checks for your network environment:**

1. Select **Security > Firewall > Attack Checks**. The Attack Checks screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced
Help
Apply
Reset

Attack Checks

WAN Security Checks

□ Respond to Ping on Internet Ports

☑ Enable Stealth Mode

□ Block TCP flood

LAN Security Checks

□ Block UDP flood

□ Disable Ping Reply on LAN Ports

VPN Pass through

☑ IPsec

☑ PPTP

☑ L2TP

Multicast Pass through

☑ Enable IGMP Pass through

Figure 56.

2. Enter the settings as explained in the following table:

Table 20. Attack Checks screen settings

Setting	Description
WAN Security Checks	
Respond to Ping on Internet Ports	Select the **Respond to Ping on Internet Ports** check box to enable the VPN firewall to respond to a ping from the Internet. A ping can be used as a diagnostic tool. Keep this check box cleared unless you have a specific reason to enable the VPN firewall to respond to a ping from the Internet.
Enable Stealth Mode	Select the **Enable Stealth Mode** check box (which is the default setting) to prevent the VPN firewall from responding to port scans from the WAN, thus making it less susceptible to discovery and attacks.
Block TCP flood	Select the **Block TCP flood** check box to enable the VPN firewall to drop all invalid TCP packets and to protect the VPN firewall from a SYN flood attack. A SYN flood is a form of denial of service attack in which an attacker sends a succession of SYN (synchronize) requests to a target system. When the system responds, the attacker does not complete the connections, thus leaving the connection half-open and flooding the server with SYN messages. No legitimate connections can then be made. By default, the **Block TCP flood** check box is cleared.

Table 20. Attack Checks screen settings (continued)

Setting	Description
LAN Security Checks.	
Block UDP flood	Select the **Block UDP flood** check box to prevent the VPN firewall from accepting more than 20 simultaneous, active UDP connections from a single device on the LAN. By default, the **Block UDP flood** check box is cleared. A UDP flood is a form of denial of service attack that can be initiated when one device sends a large number of UDP packets to random ports on a remote host. As a result, the distant host does the following: 1. Checks for the application listening at that port. 2. Sees that no application is listening at that port. 3. Replies with an ICMP Destination Unreachable packet. When the victimized system is flooded, it is forced to send many ICMP packets, eventually making it unreachable by other clients. The attacker might also spoof the IP address of the UDP packets, ensuring that the excessive ICMP return packets do not reach him, thus making the attacker’s network location anonymous.
Disable Ping Reply on LAN Ports	Select the **Disable Ping Reply on LAN Ports** check box to prevent the VPN firewall from responding to a ping on a LAN port. A ping can be used as a diagnostic tool. Keep this check box cleared unless you have a specific reason to prevent the VPN firewall from responding to a ping on a LAN port.
VPN Pass through	
IPSec PPTP L2TP	When the VPN firewall functions in NAT mode, all packets going to the remote VPN gateway are first filtered through NAT and then encrypted per the VPN policy. For example, if a VPN client or gateway on the LAN side of the VPN firewall wants to connect to another VPN endpoint on the WAN side (placing the VPN firewall between two VPN endpoints), encrypted packets are sent to the VPN firewall. Because the VPN firewall filters the encrypted packets through NAT, the packets become invalid unless you enable the VPN Pass through feature. To enable the VPN tunnel to pass the VPN traffic without any filtering, select any or all of the following check boxes: • **IPSec**. Disables NAT filtering for IPSec tunnels. • **PPTP**. Disables NAT filtering for PPTP tunnels. • **L2TP**. Disables NAT filtering for L2TP tunnels. By default, all three check boxes are selected.
Multicast Pass through	
Enable IGMP Pass through	IP multicast pass-through allows multicast packets that originate in the WAN subnet, such as packets from a media streaming or gaming application, to be forwarded to the LAN subnet. Internet Group Management Protocol (IGMP) is used to support multicast between IP hosts and their adjacent neighbors. Select the **Enable IGMP Pass through** check box to enable IP multicast pass-through. By default, IP multicast pass-through is enabled.

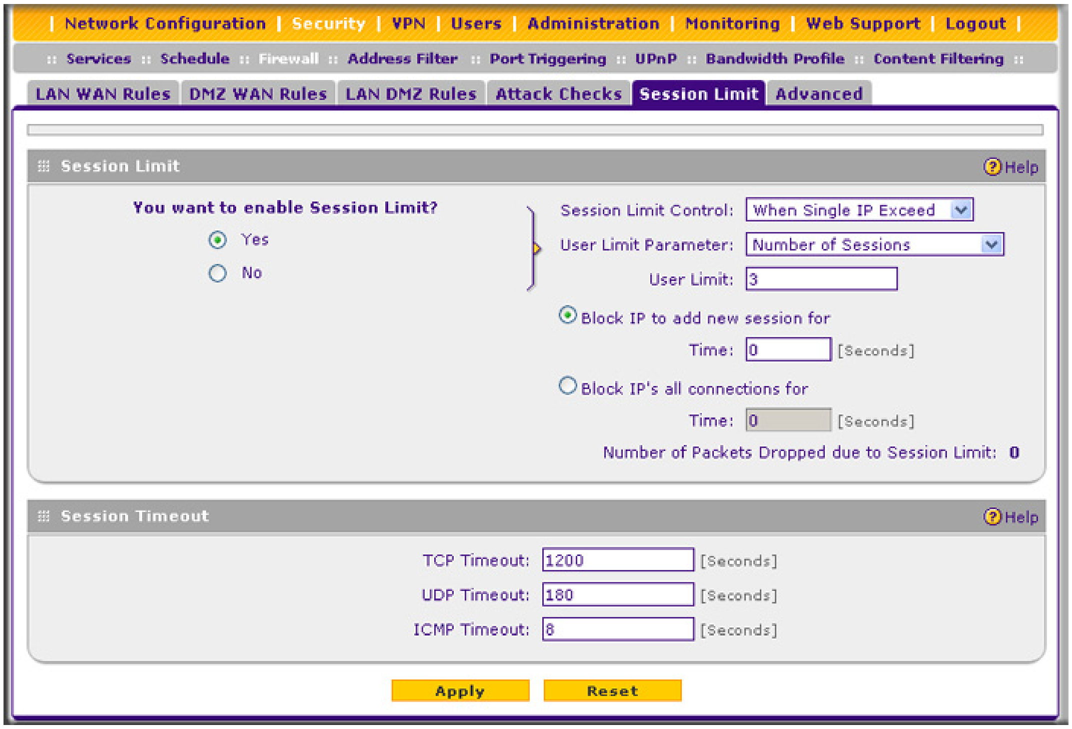
3. Click **Apply** to save your settings.

Set Session Limits

The session limits feature allows you to specify the total number of sessions that are allowed, per user, over an IP connection across the VPN firewall. The session limits feature is disabled by default.

➢ To enable and configure session limits:

1. Select **Security > Firewall > Session Limit**. The Session Limit screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced
Help
Help
Apply
Reset

Session Limit

You want to enable Session Limit?

● Yes

○ No

Session Limit Control: When Single IP Exceed

User Limit Parameter: Number of Sessions

User Limit: 3

● Block IP to add new session for

Time: 0 [Seconds]

○ Block IP's all connections for

Time: 0 [Seconds]

Number of Packets Dropped due to Session Limit: 0

Session Timeout

TCP Timeout: 1200 [Seconds]

UDP Timeout: 180 [Seconds]

ICMP Timeout: 8 [Seconds]

Figure 57.

2. Click the **Yes** radio button under Do you want to enable Session Limit?

3. Enter the settings as explained in the following table:

Table 21. Session Limit screen settings

Setting	Description
Session Limit	
Session Limit Control	From the drop-down list, select one of the following options: • **When single IP exceeds**. When the limit is reached, no new session is allowed from the IP address. A new session is allowed only when an existing session is terminated or times out. • **Single IP Cannot Exceed**. When the limit is reached, no new session is allowed from the IP address for a specified period or all sessions from the IP address are terminated and new sessions are blocked for a specified period. You need to specify the action and period by selecting one of the following radio buttons: - **Block IP to add new session for**. No new session is allowed from the IP address for a period. In the time field, specify the period in seconds. - **Block IP's all connections for**. All sessions from the IP address are terminated and new sessions are blocked for a period. In the time field, specify the period in seconds.
User Limit Parameter	From the User Limit Parameter drop-down list, select one of the following options: • **Percentage of Max Sessions**. A percentage of the total session connection capacity of the VPN firewall. • **Number of Sessions**. An absolute number of maximum sessions.
User Limit	Enter a number to indicate the user limit. The default value is 3. If the User Limit Parameter is set to Percentage of Max Sessions, the number specifies the maximum number of sessions that are allowed from a single-source device as a percentage of the total session connection capacity of the VPN firewall. (The session limit is per-device based.) If the User Limit Parameter is set to Number of Sessions, the number specifies an absolute value. **Note:** Some protocols such as FTP and RSTP create two sessions per connection, which should be considered when configuring a session limit.
Total Number of Packets Dropped due to Session Limit	This is a nonconfigurable counter that displays the total number of dropped packets when the session limit is reached.
Session Timeout	
TCP Timeout	For each protocol, specify a time-out in seconds. A session expires if no data for the session is received for the duration of the time-out period. The default time-out periods are 1200 seconds for TCP sessions, 180 seconds for UDP sessions, and 8 seconds for ICMP sessions.
UDP Timeout	
ICMP Timeout	

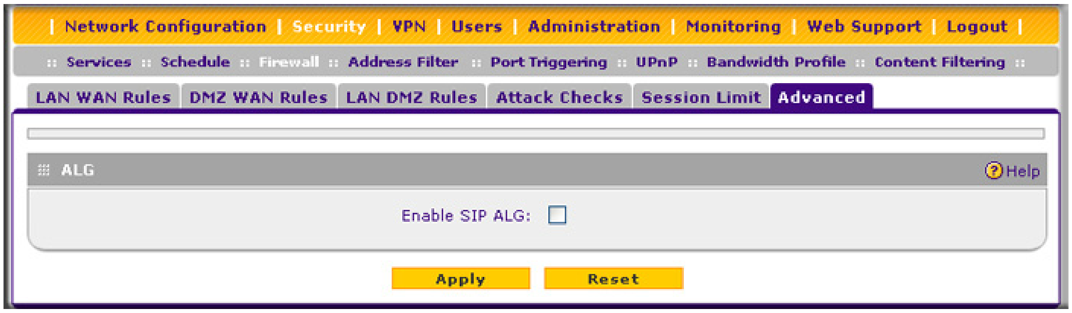
4. Click **Apply** to save your settings.

Manage the Application Level Gateway for SIP Sessions

The application level gateway (ALG) facilitates multimedia sessions such as voice over IP (VoIP) sessions that use the Session Initiation Protocol (SIP) across the firewall and provides support for multiple SIP clients. ALG support for SIP is disabled by default.

➢ **To enable ALG for SIP:**

1. Select **Security > Firewall > Advanced**. The Advanced screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
LAN WAN Rules
DMZ WAN Rules
LAN DMZ Rules
Attack Checks
Session Limit
Advanced
ALG
Help
Apply
Reset

Enable SIP ALG: □

Figure 58.

2. Select the **Enable SIP ALG** check box.
3. Click **Apply** to save your settings.

Create Services, QoS Profiles, and Bandwidth Profiles

When you create inbound and outbound firewall rules, you use firewall objects such as services, QoS profiles, bandwidth profiles, and schedules to narrow down the firewall rules:

- **Services**. A service narrows down the firewall rule to an application and a port number. For information about adding services and IP groups, see *Add Customized Services* on page 112 and *Create IP Groups* on page 114.
- **QoS profiles**. A Quality of Service (QoS) profile defines the relative priority of an IP packet for traffic that matches the firewall rule. For information about creating QoS profiles, see *Create Quality of Service (QoS) Profiles* on page 116.
- **Bandwidth profiles**. A bandwidth profile allocates and limits traffic bandwidth for the LAN users to which a firewall rule is applied. For information about creating bandwidth profiles, see *Create Bandwidth Profiles* on page 118.

Note: A schedule narrows down the period during which a firewall rule is applied. For information about specifying schedules, see *Set a Schedule to Block or Allow Specific Traffic* on page 121.

Add Customized Services

Services are functions performed by server computers at the request of client computers. You can configure up to 125 custom services.

For example, web servers serve web pages, time servers serve time and date information, and game hosts serve data about other players’ moves. When a computer on the Internet sends a request for service to a server computer, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (web server) request.

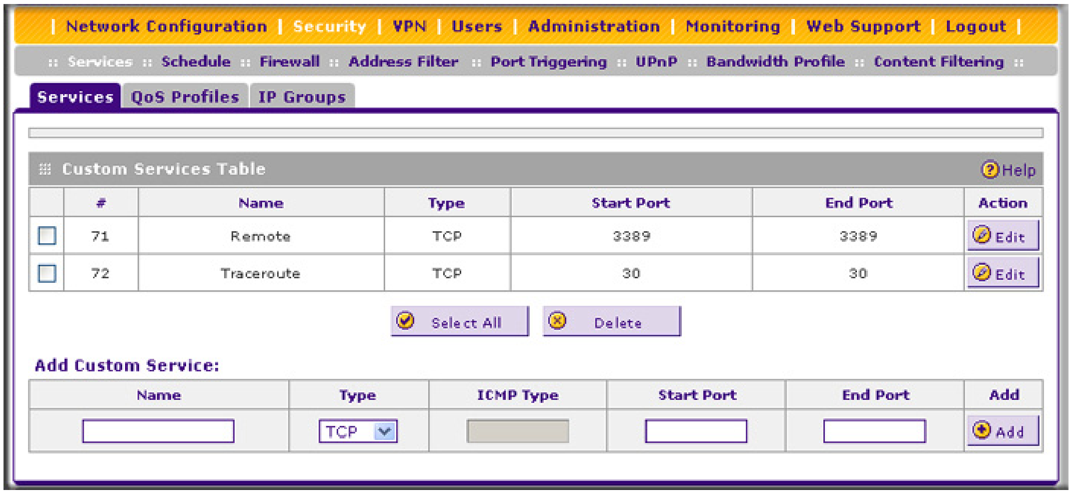
The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC 1700, *Assigned Numbers*. Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application.

Although the VPN firewall already holds a list of many service port numbers, you are not limited to these choices. Use the Services screen to add additional services and applications to the list for use in defining firewall rules. The Services screen shows a list of services that you have defined, as shown in *Figure 59,* .

To define a new service, first you need to determine which port number or range of numbers is used by the application. This information can usually be determined by contacting the publisher of the application or from user groups of newsgroups. When you have the port number information, you can enter it on the Services screen.

➢ To add a customized service:

1. Select **Security > Services**. The Services submenu tabs display, with the Services screen in view. The screen displays the Custom Services Table with the user-defined services. (The following figure shows some examples.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Services
QoS Profiles
IP Groups
Help
Select All
Delete

Custom Services Table

	#	Name	Type	Start Port	End Port	Action
□	71	Remote	TCP	3389	3389	Edit
□	72	Traceroute	TCP	30	30	Edit

Add Custom Service:

Name	Type	ICMP Type	Start Port	End Port	Add
	TCP				Add

Figure 59.

2. In the Add Customer Service section of the screen, enter the settings as explained in the following table:

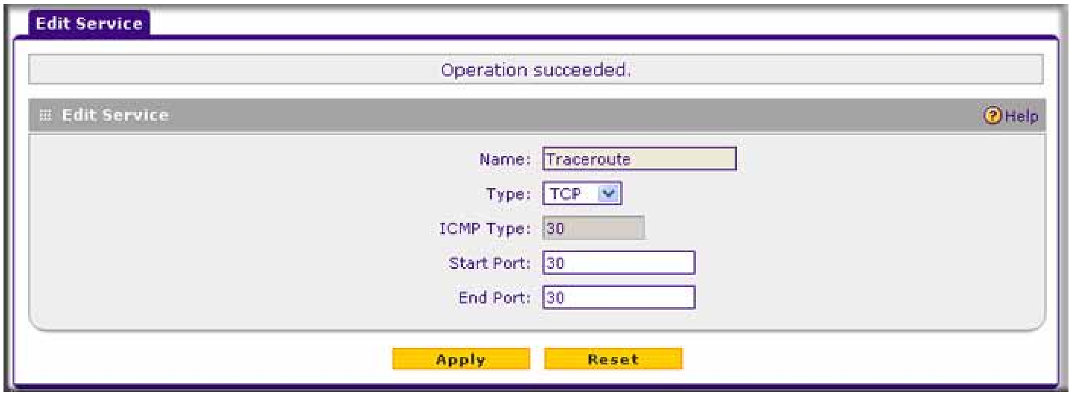
Table 22. Services screen settings

Setting	Description
Name	A descriptive name of the service for identification and management purposes.
Type	From the Type drop-down list, select the Layer 3 protocol that the service uses as its transport protocol: • **TCP** • **UDP** • **ICMP**
ICMP Type	A numeric value that can range between 0 and 40. For a list of ICMP types, see *http://www.iana.org/assignments/icmp-parameters*. This field is enabled only when you select ICMP from the Type drop-down list.
Start Port	The first TCP or UDP port of a range that the service uses. This field is enabled only when you select TCP or UDP from the Type drop-down list.
Finish Port	The first TCP or UDP port of a range that the service uses. If the service uses only a single port number, enter the same number in the Start Port and Finish Port fields. This field is enabled only when you select TCP or UDP from the Type drop-down list.

3. Click **Apply** to save your settings. The new custom service is added to the Custom Services Table.

➢ To edit a service:

1. In the Custom Services table, click the **Edit** table button to the right of the service that you want to edit. The Edit Service screen displays.



Operation succeeded.

Name: Traceroute
Type: TCP
ICMP Type: 30
Start Port: 30
End Port: 30

Figure 60.

2. Modify the settings that you wish to change (see the previous table).
3. Click **Apply** to save your changes. The modified service is displayed in the Custom Services Table.

➢ **To delete one or more services:**

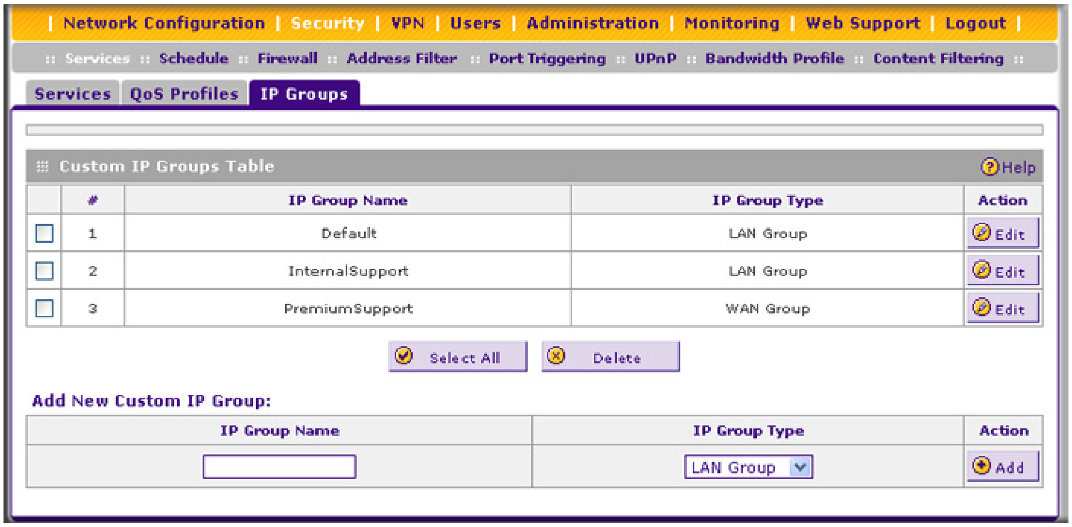
1. In the Custom Services table, select the check box to the left of the service that you want to disable, or click the **Select All** table button to select all services.
2. Click the **Delete** table button.

Create IP Groups

An IP group contains a collection of individual IP addresses that do not need to be within the same IP address range. You specify an IP group as either a LAN group or WAN group and use the group as a firewall object to which you apply a firewall rule.

➢ **To create an IP group:**

1. Select Security > Services > IP Groups. The IP Groups screen displays. (The following figure shows three groups in the Custom IP Groups table as an example.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Services
QoS Profiles
IP Groups
Help
Select All
Delete
Add

Custom IP Groups Table

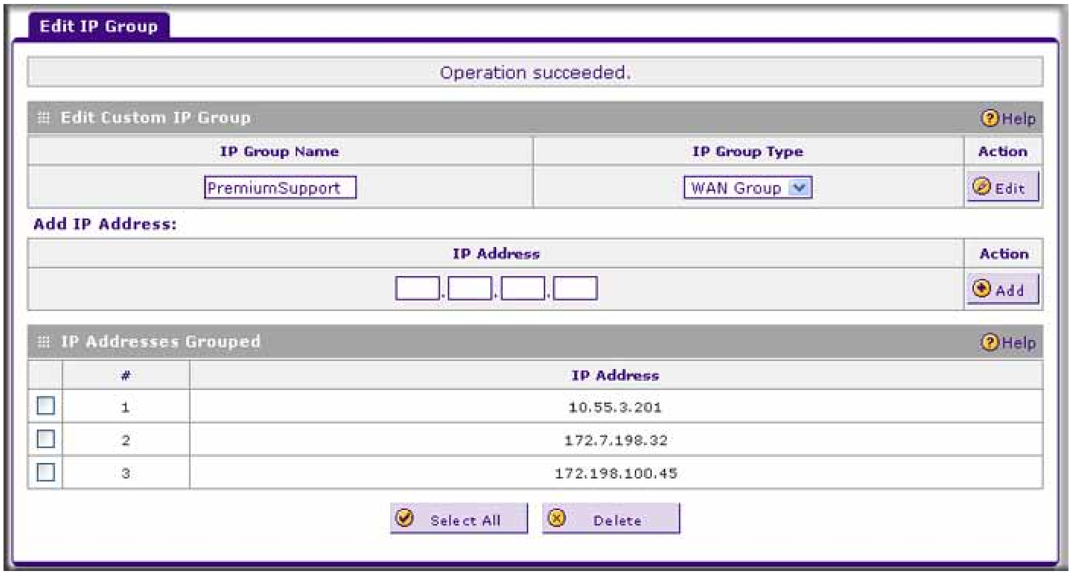
	#	IP Group Name	IP Group Type	Action
□	1	Default	LAN Group	Edit
□	2	InternalSupport	LAN Group	Edit
□	3	PremiumSupport	WAN Group	Edit

Add New Custom IP Group:

IP Group Name	IP Group Type	Action
	LAN Group	Add

Figure 61.

2. In the Add New Custom IP Group section of the screen, do the following:
   - In the IP Group Name field, enter a name for the group.
   - From the IP Group Type drop-down list, select **LAN Group** or **WAN Group**.
3. Click **Apply** to save your changes. The new IP group is displayed in the Custom IP Groups table.
4. In the Custom IP Groups table, click the **Edit** table button to the right of the IP group that you just created. The Edit IP Group screen displays. (The following figure shows three IP addresses in the IP Addresses Grouped table as an example.)



Operation succeeded.

IP Group Name	IP Group Type	Action
PremiumSupport	WAN Group	Edit

IP Address	Action
. . .	Add

	#	IP Address
□	1	10.55.3.201
□	2	172.7.198.32
□	3	172.198.100.45

Figure 62.

5. In the IP Address fields, type an IP address.
6. Click the **Add** table button to add the IP address to the IP Addresses Grouped table.
7. Repeat the previous two steps to add more IP addresses to the IP Addresses Grouped table.
8. Click the **Edit** table button to return to IP Groups screen.

➤ To edit an IP group:

1. In the Custom IP Groups table, click the **Edit** table button to the right of the IP group that you want to edit. The Edit IP Group screen displays.
2. In the Edit New Custom IP Group section of the screen, modify the settings that you wish to change:
   - You can change the group name.
   - You can change the group type.
   - You can delete an IP address from the IP Addresses Grouped table by selecting the check box to the left of the IP address that you want to delete and then clicking the **Delete** table button. You can delete all IP addresses by selecting the **Select All** table button and clicking the **Delete** table button.
   - You can add IP addresses to the IP Addresses Grouped table (see *step 4*, *step 5*, and *step 6* in the previous procedure).
3. Click the **Edit** table button to return to IP Groups screen.

➤ To delete an IP group:

1. In the Custom IP Groups table, select the check box to the left of the IP group that you want to delete, or click the **Select All** table button to select all groups.
2. Click the **Delete** table button.

Create Quality of Service (QoS) Profiles

A Quality of Service (QoS) profile defines the relative priority of an IP packet when multiple connections are scheduled for simultaneous transmission on the VPN firewall. A QoS profile becomes active only when it is associated with a nonblocking inbound or outbound firewall rule and traffic matching the firewall rule flows through the router.

After you have created a QoS profile, you can assign the QoS profile to firewall rules on the following screens:

- Add LAN WAN Outbound Services screen (see *Figure 43* on page 93).
- Add LAN WAN Inbound Services screen (see *Figure 44* on page 94).
- Add DMZ WAN Outbound Services screen (see *Figure 46* on page 96).
- Add DMZ WAN Inbound Services screen (see *Figure 47* on page 97).

Priorities are defined by the *Type of Service (ToS) in the Internet Protocol Suite standards*, RFC 1349.

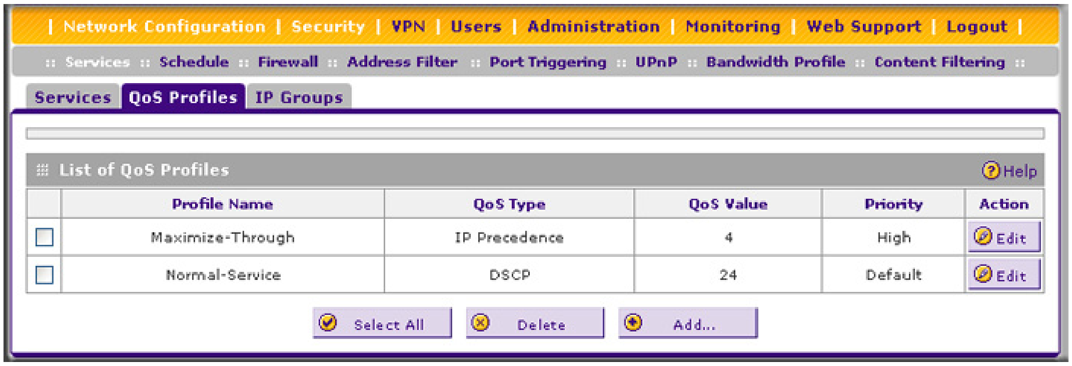
There is no default QoS profile on the VPN firewall. Following are examples of QoS profiles that you *could* create:

- Normal service profile. Used when no special priority is given to the traffic. You would typically mark the IP packets for services with this priority with a ToS value of 0.
- Minimize-cost profile. Used when data needs to be transferred over a link that has a lower cost. You would typically mark the IP packets for services with this priority with a ToS value of 1.
- Maximize-reliability profile. Used when data needs to travel to the destination over a reliable link and with little or no retransmission. You would typically mark the IP packets for services with this priority with a ToS value of 2.
- Maximize-throughput profile. Used when the volume of data transferred during an interval is important even if the latency over the link is high. You would typically mark the IP packets for services with this priority with a ToS value of 3 or 4.
- Minimize-delay profile. Used when the time required (latency) for the packet to reach the destination needs to be low. You would typically mark the IP packets for services with this priority with a ToS value of 7.

Note: This document assumes that you are familiar with QoS concepts such QoS priority queues, IP precedence, DHCP, and their values.

➤ **To create a QoS profile:**

1. Select **Security > Services > QoS Profiles**. The QoS Profiles screen displays. (The following figure shows some profiles in the List of QoS Profiles table as an example.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Services
QoS Profiles
IP Groups
Help
Edit
Select All
Delete
Add...

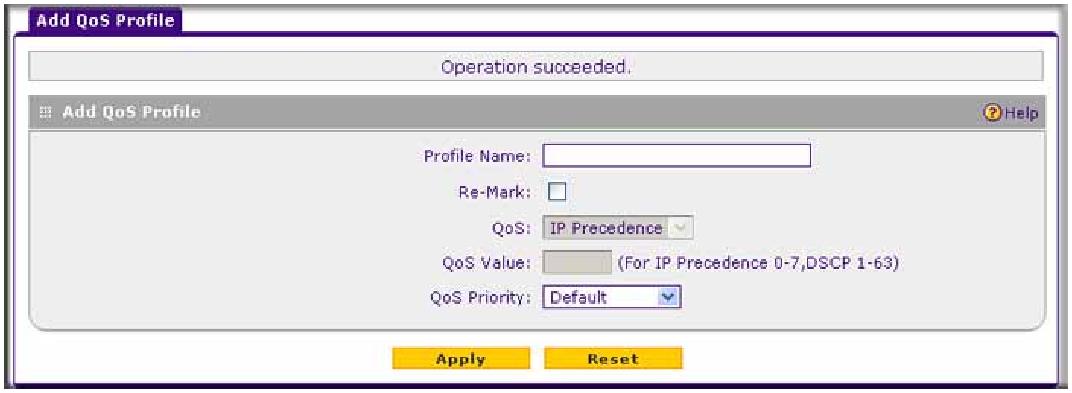
List of QoS Profiles

	Profile Name	QoS Type	QoS Value	Priority	Action
□	Maximize-Through	IP Precedence	4	High	Edit
□	Normal-Service	DSCP	24	Default	Edit

Figure 63.

The screen displays the List of QoS Profiles table with the user-defined profiles.

2. Under the List of QoS Profiles table, click the **Add** table button. The Add QoS Profile screen displays:



Operation succeeded.

Add QoS Profile

Profile Name:

Re-Mark: □

QoS: IP Precedence

QoS Value: (For IP Precedence 0-7,DSCP 1-63)

QoS Priority: Default

Figure 64.

3. Enter the settings as explained in the following table.

Table 23. Add QoS Profile screen settings

Setting	Description	
Profile Name	A descriptive name of the QoS profile for identification and management purposes.	
Re-Mark	Select the **Re-Mark** check box to set the differentiated services (DiffServ) mark in the Type of Service (ToS) byte of an IP header by specifying the QoS type (IP precedence or DHCP) and QoS value. If you clear the Re-Mark check box (which is the default setting), the QoS profile is specified only by the QoS priority.	
	QoS (Type)	From the QoS drop-down list, select one of the following traffic classification methods: • **IP Precedence**. A legacy method that sets the priority in the ToS byte of an IP header. • **DSCP**. A method that sets the Differentiated Services Code Point (DSCP) in the Differentiated Services (DS) field (which is the same as the ToS byte) of an IP header.

Table 23. Add QoS Profile screen settings (continued)

Setting	Description	
Re-Mark (continued)	QoS Value	The QoS value in the ToS or Diffserv byte of an IP header. The QoS value that you enter depends on your selection from the QoS drop-down list: • For IP Precedence, select a value from 0 to 7. • For DSCP, select a value from 0 to 63.
QoS Priority	The QoS priority represents the classification level of the packet among the priority queues within the VPN firewall. If you select **Default**, packets are mapped based on the ToS bits in their IP headers. From the QoS Priority drop-down list, select one of the following priority queues: • **Default** • **High** • **Medium High** • **Medium** • **Low**	

4. Click **Apply** to save your settings. The new QoS profile is added to the List of QoS Profiles table.

➢ **To edit a QoS profile:**

1. In the List of QoS Profiles table, click the **Edit** table button to the right of the QoS profile that you want to edit. The Edit QoS Profile screen displays.
2. Modify the settings that you wish to change (see the previous table).
3. Click **Apply** to save your changes. The modified QoS profile is displayed in the List of QoS Profiles table.

➢ **To delete a QoS profile:**

1. In the List of QoS Profiles table, select the check box to the left of the QoS profile that you want to delete, or click the **Select All** table button to select all profiles.
2. Click the **Delete** table button.

Create Bandwidth Profiles

Bandwidth profiles determine the way in which data is communicated with the hosts. The purpose of bandwidth profiles is to provide a method for allocating and limiting traffic, thus allocating LAN users sufficient bandwidth while preventing them from consuming all the bandwidth on your WAN link.

For outbound traffic, you can apply bandwidth profiles on the available WAN interfaces in both the single WAN port mode and auto-rollover mode, and in load balancing mode on the interface that you specify. For inbound traffic, you can apply bandwidth profiles to a LAN interface for all WAN modes. Bandwidth profiles do not apply to the DMZ interface.

For example, when a new connection is established by a device, the device locates the firewall rule corresponding to the connection:

- If the rule has a bandwidth profile specification, the device creates a bandwidth class in the kernel.
- If multiple connections correspond to the same firewall rule, the connections all share the same bandwidth class.

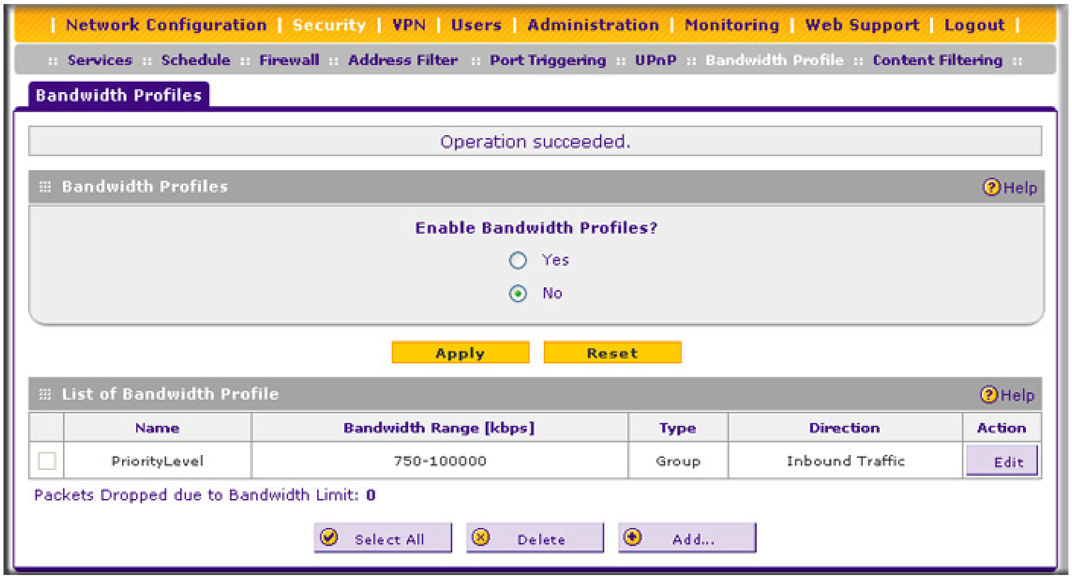
An exception occurs for an individual bandwidth profile if the classes are per-source IP address classes. The source IP address is the IP address of the first packet that is transmitted for the connection. So for outbound firewall rules, the source IP address is the LAN-side IP address; for inbound firewall rules, the source IP address is the WAN-side IP address. The class is deleted when all the connections that are using the class expire.

After you have created a bandwidth profile, you can assign the bandwidth profile to firewall rules on the following screens:

- Add LAN WAN Outbound Services screen (see *Figure 43* on page 93).
- Add LAN WAN Inbound Services screen (see *Figure 44* on page 94).

➢ To add and enable a bandwidth profile:

1. Select **Security > Bandwidth Profile**. The Bandwidth Profiles screen displays. (See the following figure, which shows one profile in the List of Bandwidth Profiles table as an example.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Bandwidth Profiles
Help
Apply
Reset
Help
Select All
Delete
Add...

Operation succeeded.

Bandwidth Profiles

Enable Bandwidth Profiles?

○ Yes

● No

List of Bandwidth Profile

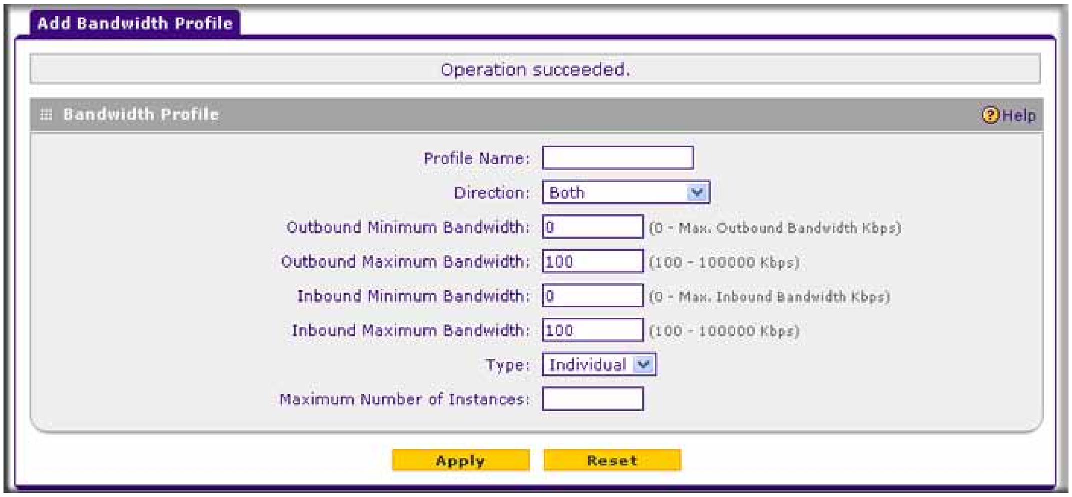
	Name	Bandwidth Range [kbps]	Type	Direction	Action
□	PriorityLevel	750-100000	Group	Inbound Traffic	Edit

Packets Dropped due to Bandwidth Limit: **0**

Figure 65.

The screen displays the List of Bandwidth Profiles table with the user-defined profiles.

2. Under the List of Bandwidth Profiles table, click the **Add** table button. The Add Bandwidth Profile screen displays:



Add Bandwidth Profile

Operation succeeded.

Bandwidth Profile

Profile Name:

Direction: Both

Outbound Minimum Bandwidth: 0 (0 - Max. Outbound Bandwidth Kbps)

Outbound Maximum Bandwidth: 100 (100 - 100000 Kbps)

Inbound Minimum Bandwidth: 0 (0 - Max. Inbound Bandwidth Kbps)

Inbound Maximum Bandwidth: 100 (100 - 100000 Kbps)

Type: Individual

Maximum Number of Instances:

Figure 66.

3. Enter the settings as explained in the following table:

Table 24. Add Bandwidth Profile screen settings

Setting	Description	
Profile Name	A descriptive name of the bandwidth profile for identification and management purposes.	
Direction	From the Direction drop-down list, select the direction in which the bandwidth profile is applied: • **Outbound Traffic**. The bandwidth profile is applied only to outbound traffic. Specify the outbound minimum and maximum bandwidths. • **Inbound Traffic**. The bandwidth profile is applied only to inbound traffic. Specify the inbound minimum and maximum bandwidths. • **Both**. The bandwidth profile is applied both to outbound and inbound traffic. Specify both the outbound and inbound minimum and maximum bandwidths.	
	Outbound Minimum Bandwidth	The outbound minimum allocated bandwidth in Kbps. The default setting is 0 Kbps.
	Outbound Maximum Bandwidth	The outbound maximum allowed bandwidth in Kbps. The default setting is 100 Kbps (you cannot configure less than 100 Kbps); the maximum allowable bandwidth is 100000 Kbps.
	Inbound Minimum Bandwidth	The inbound minimum allocated bandwidth in Kbps. The default setting is 0 Kbps.
	Inbound Maximum Bandwidth	The inbound maximum allowed bandwidth in Kbps. The default setting is 100 Kbps (you cannot configure less than 100 Kbps); the maximum allowable bandwidth is 100000 Kbps.

Table 24. Add Bandwidth Profile screen settings (continued)

Setting	Description	
Type	From the Type drop-down list, select the type for the bandwidth profile: • **Group**. The profile applies to all users, that is, all user share the available bandwidth. • **Individual**. The profile applies to an individual user, that is, each user can use the available bandwidth.	
	Maximum Number of Instances	If you select Individual from the Type drop-down list, you need to specify the maximum number of class instances that can be created by the individual bandwidth profile. **Note:** If the number of users exceeds the configured number of instances, the same bandwidth is shared among all the users of that bandwidth profile.

4. Click **Apply** to save your settings. The new bandwidth profile is added to the List of Bandwidth Profiles table.
5. In the Bandwidth Profiles section of the screen, select the **Yes** radio button under Enable Bandwidth Profiles? (By default the **No** radio button is selected.)
6. Click **Apply** to save your settings.

➢ **To edit a bandwidth profile:**

1. In the List of Bandwidth Profiles table, click the **Edit** table button to the right of the bandwidth profile that you want to edit. The Edit Bandwidth Profile screen displays.
2. Modify the settings that you wish to change (see the previous table).
3. Click **Apply** to save your changes. The modified bandwidth profile is displayed in the List of Bandwidth Profiles table.

➢ **To delete one or more bandwidth profiles:**

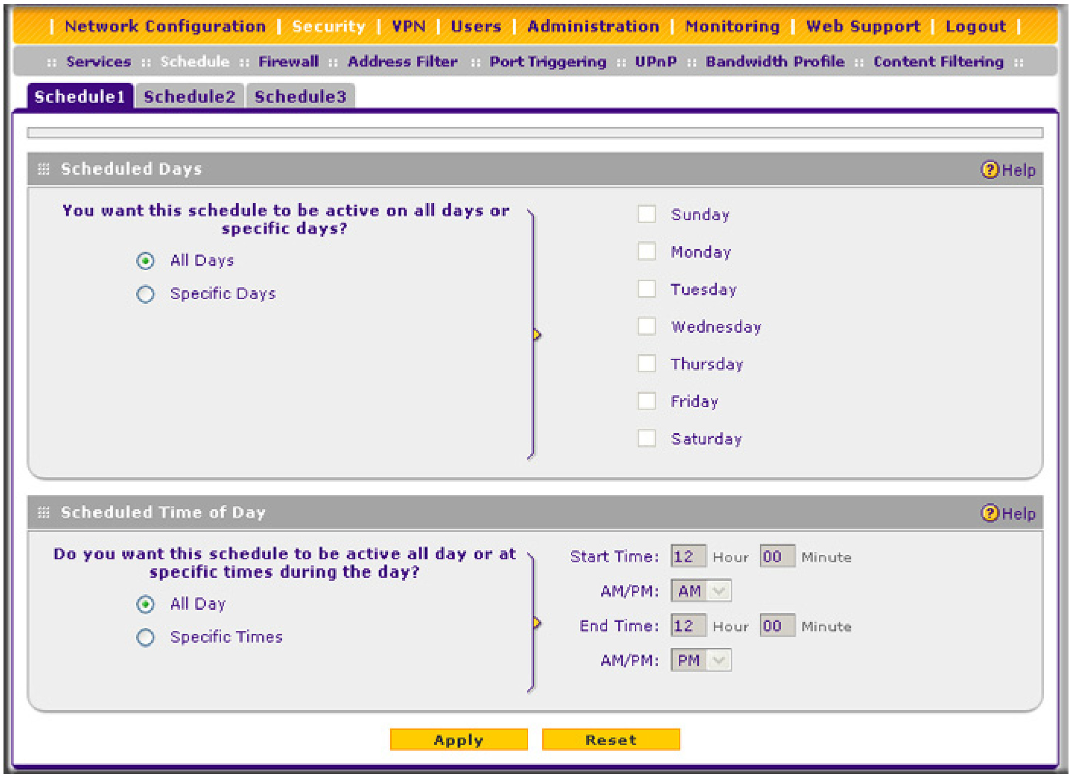
1. In the List of Bandwidth Profiles table, select the check box to the left of the bandwidth profile that you want to delete, or click the **Select All** table button to select all profiles.
2. Click the **Delete** table button to delete the selected profile or profiles.

Set a Schedule to Block or Allow Specific Traffic

Schedules define the time frames under which firewall rules can be applied. Three schedules, Schedule 1, Schedule 2, and Schedule3 can be defined, and you can select any one of these when defining firewall rules.

➢ **To set a schedule:**

1. Select **Security > Schedule**. The Schedule submenu tabs display, with the Schedule 1 screen in view:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Schedule1
Schedule2
Schedule3
Help
Help
Apply
Reset

Scheduled Days

You want this schedule to be active on all days or specific days?

● All Days
○ Specific Days

□ Sunday
□ Monday
□ Tuesday
□ Wednesday
□ Thursday
□ Friday
□ Saturday

Scheduled Time of Day

Do you want this schedule to be active all day or at specific times during the day?

● All Day
○ Specific Times

Start Time: 12 Hour 00 Minute
AM/PM: AM
End Time: 12 Hour 00 Minute
AM/PM: PM

Figure 67.

2. In the Scheduled Days section, select one of the following radio buttons:
   - **All Days**. The schedule is in effect all days of the week.
   - **Specific Days**. The schedule is active only on specific days. To the right of the radio buttons, select the check box for each day that you want the schedule to be in effect.
3. In the Scheduled Time of Day section, select one of the following radio buttons:
   - **All Day**. The schedule is in effect all hours of the selected day or days.
   - **Specific Times**. The schedule is active only during specific hours of the selected day or days. To the right of the radio buttons, fill in the Start Time and End Time fields (Hour, Minute, AM/PM) during which the schedule is in effect.
4. Click **Apply** to save your settings to Schedule 1.

Repeat these steps to set to a schedule for Schedule 2 and Schedule 3.

Content Filtering

If you want to restrict internal LAN users from access to certain sites on the Internet, you can use the VPN firewall’s content filtering and web components filtering features. By default, these features are disabled; all requested traffic from any website is allowed. If you enable one or more of these features and users try to access a blocked site, they will see a *Blocked by NETGEAR* message.

Content Filtering

The VPN firewall supports several types of content filtering:

- **Web components blocking**. You can block the following web component types: Proxy, Java, ActiveX, and cookies. Some of these components can be used by malicious websites to infect computers that access them. Even sites on the Trusted Domains list will be subject to web components blocking when the blocking of a particular web component is enabled.
    - **Proxy**. A proxy server (or simply, proxy) allows computers to route connections to other computers through the proxy, thus circumventing certain firewall rules. For example, if connections to a specific IP address are blocked by a firewall rule, the requests can be routed through a proxy that is not blocked by the rule, rendering the restriction ineffective. Enabling this feature blocks proxy servers.
    - **Java**. Blocks Java applets from being downloaded from pages that contain them. Java applets are small programs embedded in web pages that enable dynamic functionality of the page. A malicious applet can be used to compromise or infect computers. Enabling this setting blocks Java applets from being downloaded.
    - **ActiveX**. Similar to Java applets, ActiveX controls are installed on a Windows computer running Internet Explorer. A malicious ActiveX control can be used to compromise or infect computers. Enabling this setting blocks ActiveX applets from being downloaded.
    - **Cookies**. Cookies are used to store session information by websites that usually require login. However, several websites use cookies to store tracking information and browsing habits. Enabling this option filters out cookies from being created by a website.

Note: Many websites require that cookies be accepted in order for the site to be accessed correctly. Blocking cookies might interfere with useful functions provided by these websites.

- **Keyword blocking** (domain name blocking). You can specify up to 32 words that, should they appear in the website name (URL) or in a newsgroup name, will cause that site or newsgroup to be blocked by the VPN firewall.

You can apply the keywords to one or more groups. Requests from the PCs in the groups for which keyword blocking has been enabled will be blocked. Blocking does not occur for the PCs that are in the groups for which keyword blocking has not been enabled.

You can bypass keyword blocking for trusted domains by adding the exact matching domain to the list of trusted domains. Access to the domains or keywords on this list by PCs, even those in the groups for which keyword blocking has been enabled, will still be allowed without any blocking.

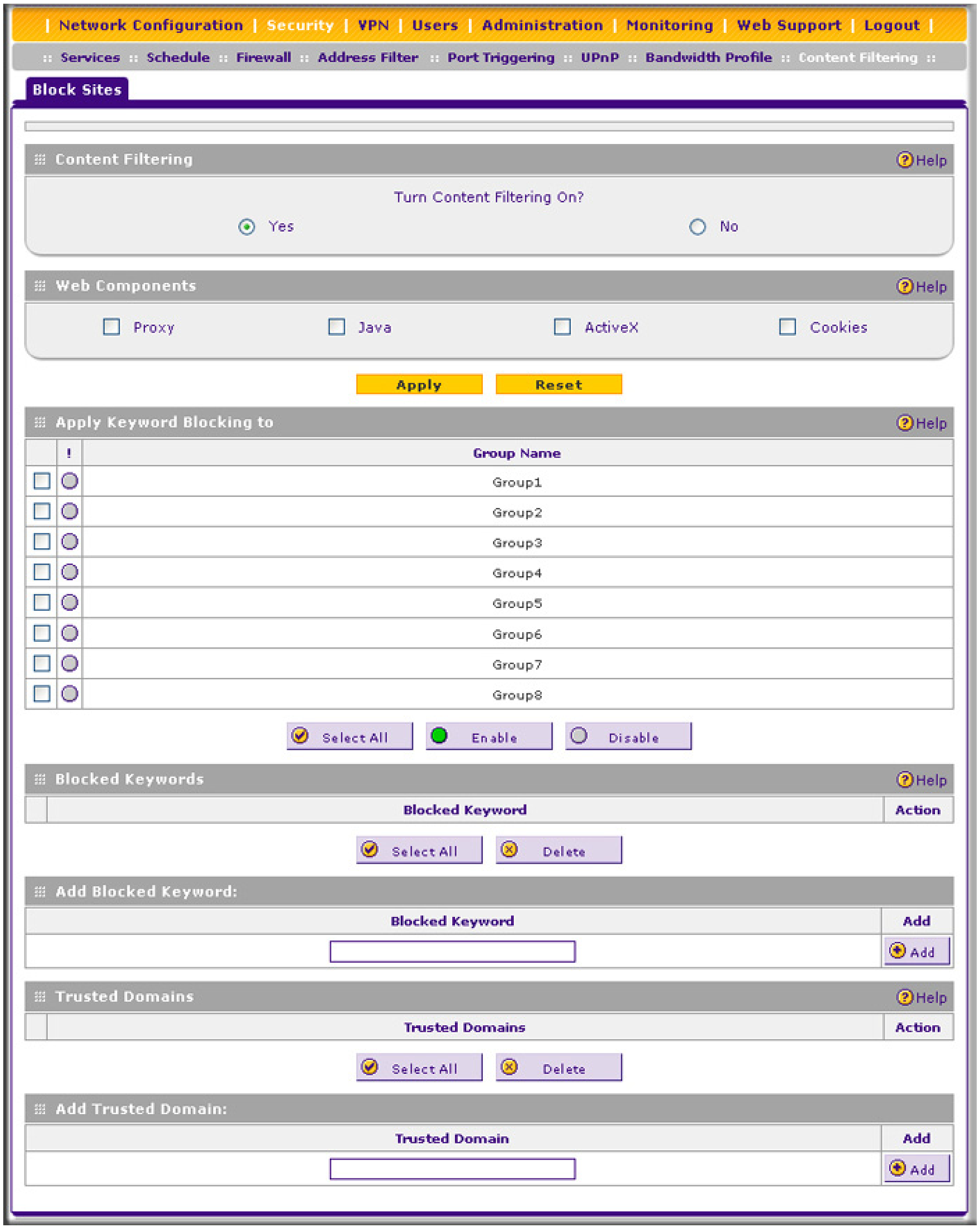
Keyword application examples:

- If the keyword XXX is specified, the URL www.zzyyqq.com/xxx.html is blocked, as is the newsgroup alt.pictures.XXX.
- If the keyword .com is specified, only websites with other domain suffixes (such as .edu or .gov) can be viewed.
- If a period (**.**) is specified as the keyword, all Internet browsing access is blocked.

Enable and Configure Content Filtering

➢ **To enable and configure content filtering:**

1. Select **Security > Content Filtering**. The Block Sites screen displays (see the following figure).
2. In the Content Filtering section, select the **Yes** radio button to enable content filtering.
3. Click **Apply** to activate the screen controls. The check boxes and fields that were masked out become available for configuration.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Block Sites
Help
Apply
Reset
Select All
Enable
Disable
Select All
Delete
Add
Select All
Delete
Add

Content Filtering

Turn Content Filtering On?

● Yes ○ No

Web Components

□ Proxy □ Java □ ActiveX □ Cookies

Apply Keyword Blocking to

	!	Group Name
□	○	Group1
□	○	Group2
□	○	Group3
□	○	Group4
□	○	Group5
□	○	Group6
□	○	Group7
□	○	Group8

Blocked Keywords

	Blocked Keyword	Action

Add Blocked Keyword:

Blocked Keyword	Add
	Add

Trusted Domains

	Trusted Domains	Action

Add Trusted Domain:

Trusted Domain	Add
	Add

Figure 68.

4. Enter the settings as explained in the following table:

Table 25. Block Sites screen settings

Setting	Description
Web Components	
Select the check boxes of any \web components that you wish to block. The web components are explained in *Content Filtering* on page 123.	
Apply Keyword Blocking to	
To apply keyword blocking to groups: 1. Select the check boxes for the groups to which you wish to apply keyword blocking, or click the **Select All** button to select all groups. 2. Click the **Enable** button to activate keyword blocking for these groups. (To deactivate keyword blocking for the selected groups, click the **Disable** button.)	
(Add) Blocked Keyword(s)	
To build your list of blocked keywords or blocked domain names: 1. In the Add Blocked Keyword section, enter a keyword or domain name in the Blocked Keyword field. 2. After each entry, click the **Add** table button. The keyword or domain name is added to the Blocked Keywords table. To edit an entry, click the **Edit** table button in the Action column adjacent to the entry.	
(Add) Trusted Domain(s)	
To build your list of trusted domains: 1. In the Add Trusted Domain section, enter a domain name in the Trusted Domains field. 2. After each entry, click the **Add** table button. The domain name is added to the Trusted Domains table. To edit an entry, click the **Edit** table button in the Action column adjacent to the entry.	

5. Click **Apply** to save your selection of web components. (The selected groups for keyword blocking are saved after you have clicked the **Enable** button; keywords and trusted domains are saved after you have added them to their respective tables.)

Enable Source MAC Filtering

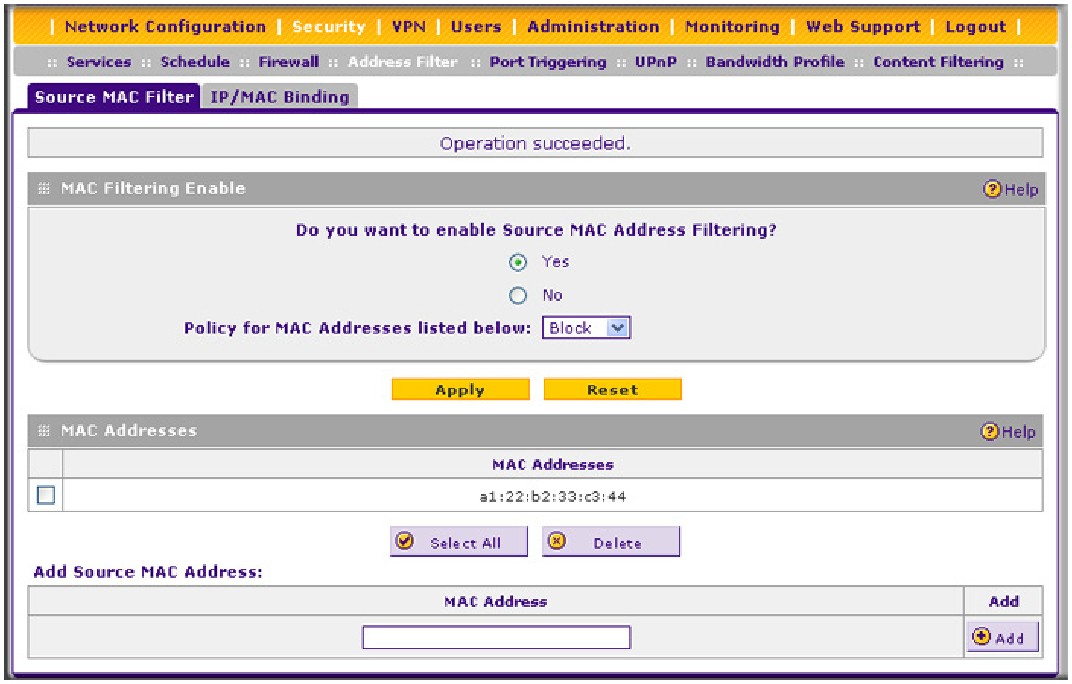
The Source MAC Filter screen enables you to permit or block traffic coming from certain known PCs or devices.

By default, the source MAC address filter is disabled. All the traffic received from PCs with any MAC address is allowed. When the source MAC address filter is enabled, depending on the selected policy, traffic is either permitted or blocked if it comes from any PCs or devices whose MAC addresses are listed in MAC Addresses table.

Note: For additional ways of restricting outbound traffic, see *Outbound Rules (Service Blocking)* on page 83.

➤ **To enable MAC filtering and add MAC addresses to be permitted or blocked:**

1. Select **Security > Address Filter**. The Address Filter submenu tabs display, with the Source MAC Filter screen in view. (The following figure shows one address in the MAC Addresses table as an example.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Source MAC Filter
IP/MAC Binding
MAC Filtering Enable
Help
Apply
Reset
MAC Addresses
Help
Select All
Delete
Add

Operation succeeded.

Do you want to enable Source MAC Address Filtering?

● Yes

○ No

Policy for MAC Addresses listed below: Block

	MAC Addresses
□	a1:22:b2:33:c3:44

Add Source MAC Address:

MAC Address	Add
	Add

Figure 69.

2. In the MAC Filtering Enable section, select the **Yes** radio button.
3. In the same section, below the radio buttons, select one of the following options from the drop-down list:
   - **Block**. Traffic coming from all addresses in the MAC Addresses table is blocked.
   - **Permit**. Traffic coming from all addresses in the MAC Addresses table is permitted.
4. Below Add Source MAC Address, build your list of source MAC addresses to be permitted or blocked by entering the first MAC address in the MAC Address field. A MAC address needs to be entered in the format xx:xx:xx:xx:xx:xx, in which x is a numeric (0 to 9) or a letter between a and f (inclusive), for example: aa:11:bb:22:cc:03.
5. Click the **Add** table button. The MAC address is added to the MAC Addresses table.
6. Click **Apply** to save your settings.

➢ **To remove one or more entries from the table:**

1. Select the check box to the left of the MAC address that you want to delete, or click the **Select All** table button to select all entries.
2. Click the **Delete** table button.

Set Up IP/MAC Bindings

IP/MAC binding allows you to bind an IP address to a MAC address and vice versa. Some PCs or devices are configured with static addresses. To prevent users from changing their static IP addresses, the IP/MAC binding feature needs to be enabled on the VPN firewall. If the VPN firewall detects packets with a matching IP address but with the inconsistent MAC address (or vice versa), the packets are dropped. If you have enabled the logging option for the IP/MAC binding feature, these packets are logged before they are dropped. The VPN firewall displays the total number of dropped packets that violate either the IP-to-MAC binding or the MAC-to-IP binding.

Note: You can bind IP addresses to MAC addresses for DHCP assignment on the LAN Groups submenu. See *Manage the Network Database* on page 68.

As an example, assume that three computers on the LAN are set up as follows:

- Host1. MAC address (00:01:02:03:04:05) and IP address (192.168.10.10)
- Host2. MAC address (00:01:02:03:04:06) and IP address (192.168.10.11)
- Host3. MAC address (00:01:02:03:04:07) and IP address (192.168.10.12)

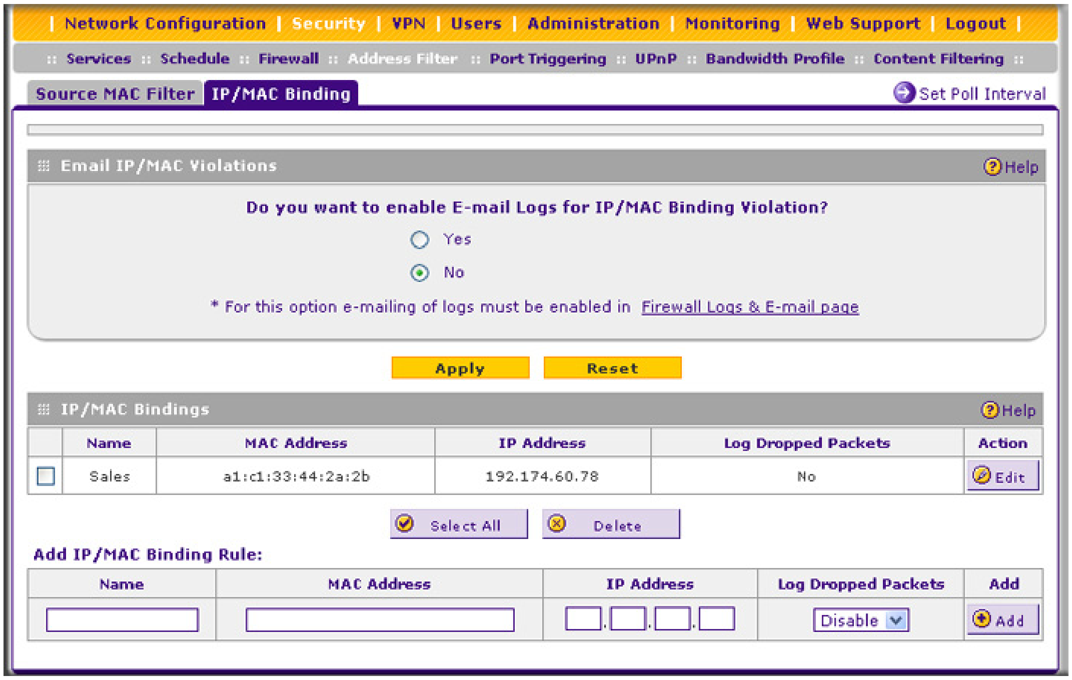
If all of the preceding host entry examples are added to the IP/MAC Bindings table, the following scenarios indicate the possible outcome.

- Host1. Matching IP address and MAC address in the IP/MAC Bindings table.
- Host2. Matching IP address but inconsistent MAC address in the IP/MAC Bindings table.
- Host3. Matching MAC address but inconsistent IP address in the IP/MAC Bindings table.

In this example, the VPN firewall blocks the traffic coming from Host2 and Host3, but allows the traffic coming from Host1 to any external network. The total count of dropped packets is displayed.

➢ **To set up IP/MAC bindings:**

1. Select **Security > Address Filter > IP/MAC Binding**. The IP/MAC Binding screen displays. (See the following figure, which shows one binding in the IP/MAC Binding table as an example.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Source MAC Filter
IP/MAC Binding
Set Poll Interval
Help
Apply
Reset
Help
Edit
Select All
Delete
Add

Email IP/MAC Violations

Do you want to enable E-mail Logs for IP/MAC Binding Violation?

○ Yes

● No

* For this option e-mailing of logs must be enabled in Firewall Logs & E-mail page

IP/MAC Bindings

	Name	MAC Address	IP Address	Log Dropped Packets	Action
□	Sales	a1:c1:33:44:2a:2b	192.174.60.78	No	Edit

Add IP/MAC Binding Rule:

Name	MAC Address	IP Address	Log Dropped Packets	Add
		. . .	Disable	Add

Figure 70.

2. Enter the settings as explained in the following table:

Table 26. IP/MAC Binding screen settings

Setting	Description
Email IP/MAC Violations	
Do you want to enable E-mail Logs for IP/MAC Binding Violation?	Select one of the following radio buttons: • **Yes.** IP/MAC binding violations are emailed. • **No**. IP/MAC binding violations are not emailed. **Note:** Click the **Firewall Logs & E-mail page** link to ensure that emailing of logs is enabled on the Email and Syslog screen (see *Activate Notification of Events, Alerts, and Syslogs* on page 269).
IP/MAC Bindings	
Name	A descriptive name of the binding for identification and management purposes.
MAC Address	The MAC address of the PC or device that is bound to the IP address.
IP Address	The IP address of the PC or device that is bound to the MAC address.
Log Dropped Packets	To log the dropped packets, select **Enable** from the drop-down list. The default setting is Disable.

3. Click the **Add** table button. The new IP/MAC rule is added to the IP/MAC Bindings table.
4. Click **Apply** to save your changes.

➤ **To edit an IP/MAC binding:**

1. In the IP/MAC Bindings table, click the **Edit** table button to the right of the IP/MAC binding that you want to edit. The Edit IP/MAC Binding screen displays.
2. Modify the settings that you wish to change (see the previous table).
3. Click **Apply** to save your changes. The modified IP/MAC binding is displayed in the IP/MAC Bindings table.

➤ **To remove one or more IP/MAC bindings from the table:**

1. Select the check box to the left of the IP/MAC binding that you want to delete, or click the **Select All** table button to select all bindings.
2. Click the **Delete** table button.

Configure Port Triggering

Port triggering allows some applications running on a LAN network to be available to external applications that would otherwise be partially blocked by the firewall. Using the port triggering feature requires that you know the port numbers used by the application.

Once configured, port triggering operates as follows:

1. A PC makes an outgoing connection using a port number that is defined in the Port Triggering Rules table.
2. The VPN firewall records this connection, opens the additional incoming port or ports that are associated with the rule in the port triggering table, and associates them with the PC.
3. The remote system receives the PC’s request and responds using the incoming port or ports that are associated with the rule in the port triggering table on the VPN firewall.
4. The VPN firewall matches the response to the previous request, and forwards the response to the PC.

Without port triggering, the response from the external application would be treated as a new connection request rather than a response to a requests from the LAN network. As such, it would be handled in accordance with the inbound port forwarding rules, and most likely would be blocked.

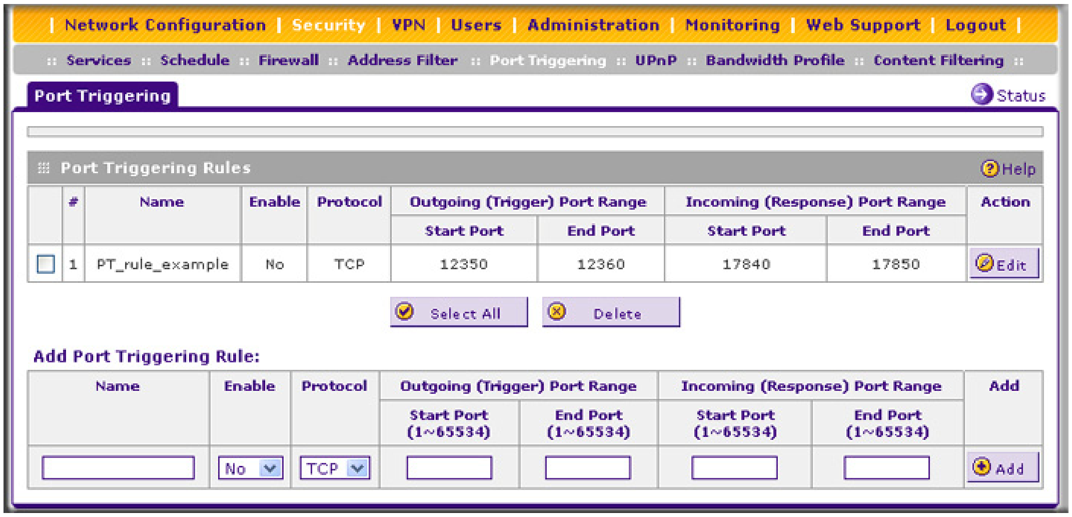
Note these restrictions on port triggering:

- Only one PC can use a port triggering application at any time.
- After a PC has finished using a port triggering application, there is a short time-out period before the application can be used by another PC. This time-out period is required so the VPN firewall can determine that the application has terminated.

Note: For additional ways of allowing inbound traffic, see *Inbound Rules (Port Forwarding)* on page 86.

To add a port triggering rule:

1. Select **Security > Port Triggering**. The Port Triggering screen displays. (See the following figure, which shows one rule in the Port Triggering Rule table as an example.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Port Triggering
Status
Port Triggering Rules
Help
Select All
Delete
Add Port Triggering Rule:

	#	Name	Enable	Protocol	Outgoing (Trigger) Port Range		Incoming (Response) Port Range		Action
					Start Port	End Port	Start Port	End Port	
□	1	PT_rule_example	No	TCP	12350	12360	17840	17850	Edit

Name	Enable	Protocol	Outgoing (Trigger) Port Range		Incoming (Response) Port Range		Add
			Start Port (1~65534)	End Port (1~65534)	Start Port (1~65534)	End Port (1~65534)	
	No	TCP					Add

Figure 71.

2. Below Add Port Triggering Rule, enter the settings as explained in the following table:

Table 27. Port Triggering screen settings

Setting	Description	
Name	A descriptive name of the rule for identification and management purposes.	
Enable	From the drop-down list, select **Yes** to enable the rule. (You can define a rule but not enable it.) The default setting is No.	
Protocol	From the drop-down list, select the protocol to which the rule applies: • **TCP.** The rule applies to an application that uses the Transmission Control Protocol (TCP). • **UDP**. The rule applies to an application that uses the User Control Protocol (UCP).	
Outgoing (Trigger) Port Range	Start Port	The start port (1–65534) of the range for triggering.
	End Port	The end port (1–65534) of the range for triggering.
Incoming (Response) Port Range	Start Port	The start port (1–65534) of the range for responding.
	End Port	The end port (1–65534) of the range for responding.

3. Click the **Add** table button. The new port triggering rule is added to the Port Triggering Rules table.

➢ To edit a port triggering rule (for example, to enable the rule):

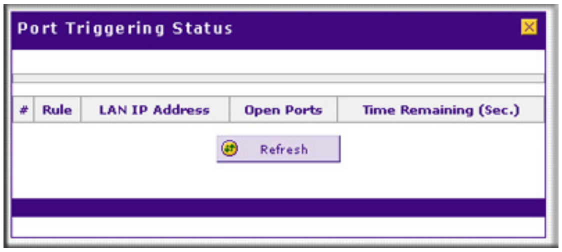
1. In the Port Triggering Rules table, click the **Edit** table button to the right of the port triggering rule that you want to edit. The Edit Port Triggering Rule screen displays.
2. Modify the settings that you wish to change (see the previous table).
3. Click **Apply** to save your changes. The modified port triggering rule is displayed in the Port Triggering Rules table.

➢ To remove one or more port-triggering rules from the table:

1. Select the check box to the left of the port-triggering rule that you want to delete, or click the **Select All** table button to select all rules.
2. Click the **Delete** table button.

➢ To display the status of the port-triggering rules:

Click the **Status** option arrow in the upper right of the Port Triggering screen. A popup window appears, displaying the status of the port triggering rules.



#	Rule	LAN IP Address	Open Ports	Time Remaining (Sec.)

Figure 72.

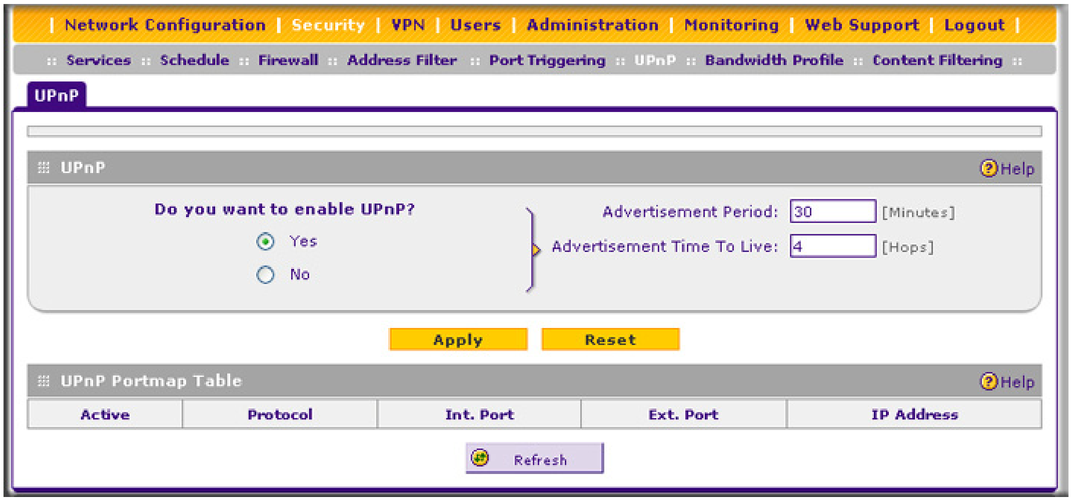
Configure Universal Plug and Play

The Universal Plug and Play (UPnP) feature enables the VPN firewall to automatically discover and configure devices when it searches the LAN and WAN.

1. Select **Security > UPnP**. The UPnP screen displays (see the following figure).

   The UPnP Portmap Table in the lower part of the screen shows the IP addresses and other settings of UPnP devices that have accessed the VPN firewall and that have been automatically detected by the VPN firewall:

   - **Active**. A Yes or No indicates if the UPnP device port that established a connection is currently active.
   - **Protocol**. Indicates the network protocol such as HTTP or FTP that is used by the device to connect to the VPN firewall.
   - **Int. Port**. Indicates if any internal ports are opened by the UPnP device.
   - **Ext. Port**. Indicates if any external ports are opened by the UPnP device.
   - **IP Address**. Lists the IP address of the UPnP device accessing the VPN firewall.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
UPnP
UPnP
Help
Apply
Reset
UPnP Portmap Table
Help
Refresh

Do you want to enable UPnP?

● Yes

○ No

Advertisement Period: 30 [Minutes]

Advertisement Time To Live: 4 [Hops]

Active	Protocol	Int. Port	Ext. Port	IP Address

Figure 73.

2. To enable the UPnP feature, select the **Yes** radio button. (The feature is disabled by default.) To disable the feature, select **No**.
3. Configure the following fields:
   - **Advertisement Period**. Enter the period in minutes that specifies how often the VPN firewall should broadcast its UPnP information to all devices within its range. The default setting is 40 minutes.
   - **Advertisement Time to Live**. Enter a number that specifies how many steps (hops) each UPnP packet is allowed to propagate before being discarded. Small values will limit the UPnP broadcast range. The default setting is 4 hops.
4. Click **Apply** to save your settings.

To refresh the contents of the UPnP Portmap Table, click **Refresh**.

Virtual Private Networking Using IPSec Connections

5

This chapter describes how to use the IP security (IPSec) virtual private networking (VPN) features of the VPN firewall to provide secure, encrypted communications between your local network and a remote network or computer. This chapter contains the following sections:

Considerations for Multi-WAN Port Systems

If two WAN ports of the VPN firewall are configured, you can enable either auto-rollover mode for increased system reliability or load balancing mode for optimum bandwidth efficiency. Your WAN mode selection impacts how the VPN features need to be configured.

The use of fully qualified domain names (FQDNs) in VPN policies is mandatory when the WAN ports function in auto-rollover mode or load balancing mode, and is also required for VPN tunnel failover. When the WAN ports function in load balancing mode, you cannot configure VPN tunnel failover. An FQDN is optional when the WAN ports function in load balancing mode if the IP addresses are static, but mandatory if the WAN IP addresses are dynamic.

See *Virtual Private Networks* on page 313 for more information about the IP addressing requirements for VPNs in the dual WAN modes. For information about how to select and configure a Dynamic DNS service for resolving FQDNs, see *Configure Dynamic DNS* on page 42. For information about WAN mode configuration, see *Configure the WAN Mode* on page 32.

The following diagrams and table show how the WAN mode selection relates to VPN configuration.

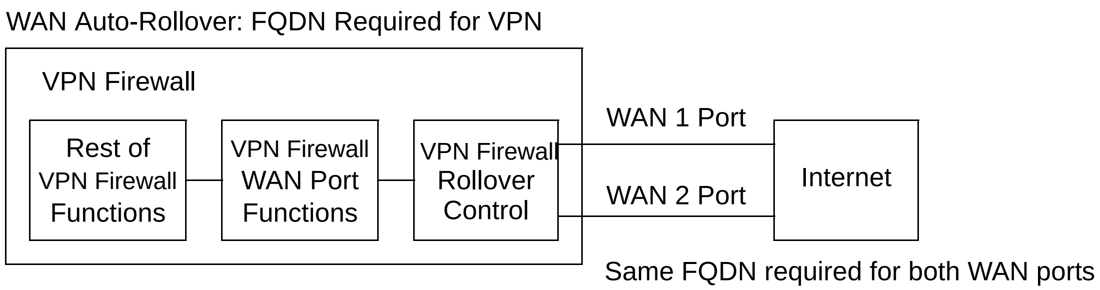

WAN Auto-Rollover: FQDN Required for VPN
VPN Firewall
Rest of VPN Firewall Functions
VPN Firewall WAN Port Functions
VPN Firewall Rollover Control
WAN 1 Port
WAN 2 Port
Internet
Same FQDN required for both WAN ports

Figure 74.

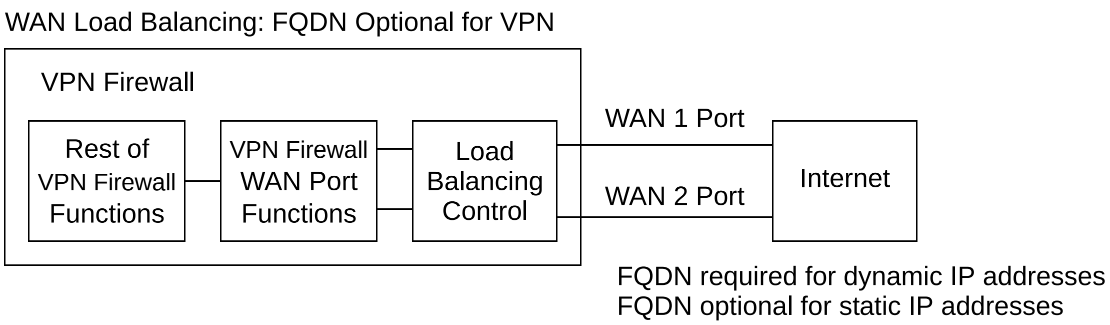

WAN Load Balancing: FQDN Optional for VPN
VPN Firewall
Rest of VPN Firewall Functions
VPN Firewall WAN Port Functions
Load Balancing Control
WAN 1 Port
WAN 2 Port
Internet
FQDN required for dynamic IP addresses
FQDN optional for static IP addresses

Figure 75.

The following table summarizes the WAN addressing requirements (FQDN or IP address) for a VPN tunnel in either dual WAN mode.

Table 28. IP Addressing for VPNs in Dual WAN Port Systems

Configuration and WAN IP address		Rollover mode[a]	Load balancing mode
VPN “Road Warrior” (client-to-gateway)	Fixed	FQDN required	FQDN Allowed (optional)
	Dynamic	FQDN required	FQDN required
VPN “Gateway-to-Gateway”	Fixed	FQDN required	FQDN Allowed (optional)
	Dynamic	FQDN required	FQDN required
VPN “Telecommuter” (client-to-gateway through a NAT router)	Fixed	FQDN required	FQDN Allowed (optional)
	Dynamic	FQDN required	FQDN required

[a] After a rollover, all tunnels need to be reestablished using the new WAN IP address.

Use the IPSec VPN Wizard for Client and Gateway Configurations

You can use the IPSec VPN Wizard to configure multiple gateway or client VPN tunnel policies.

The following section provides wizard and NETGEAR ProSafe VPN Client software configuration procedures for the following scenarios:

- Using the wizard to configure a VPN tunnel between two VPN gateways.
- Using the wizard to configure a VPN tunnel between a VPN gateway and a VPN client.

Configuring a VPN tunnel connection requires that all settings on both sides of the VPN tunnel match or mirror each other precisely, which can be a daunting task. The VPN Wizard efficiently guides you through the setup procedure with a series of questions that determine the IPSec keys and VPN policies it sets up. The VPN Wizard also configures the settings for the network connection: security association (SA), traffic selectors, authentication algorithm, and encryption. The settings that are used by the VPN Wizard are based on the recommendations of the VPN Consortium (VPNC), an organization that promotes multivendor VPN interoperability.

Create Gateway-to-Gateway VPN Tunnels with the Wizard

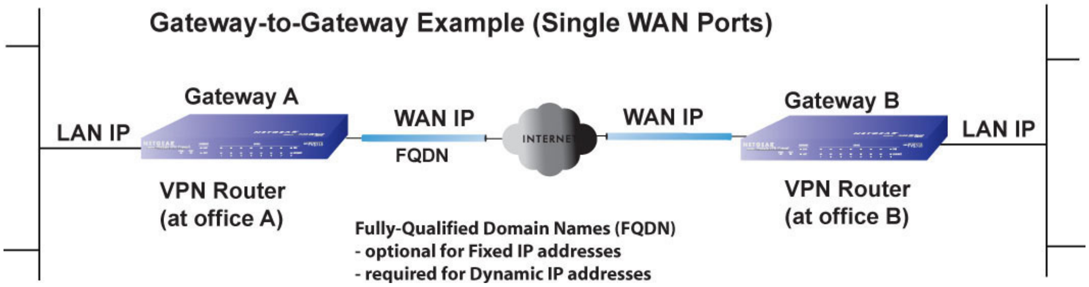
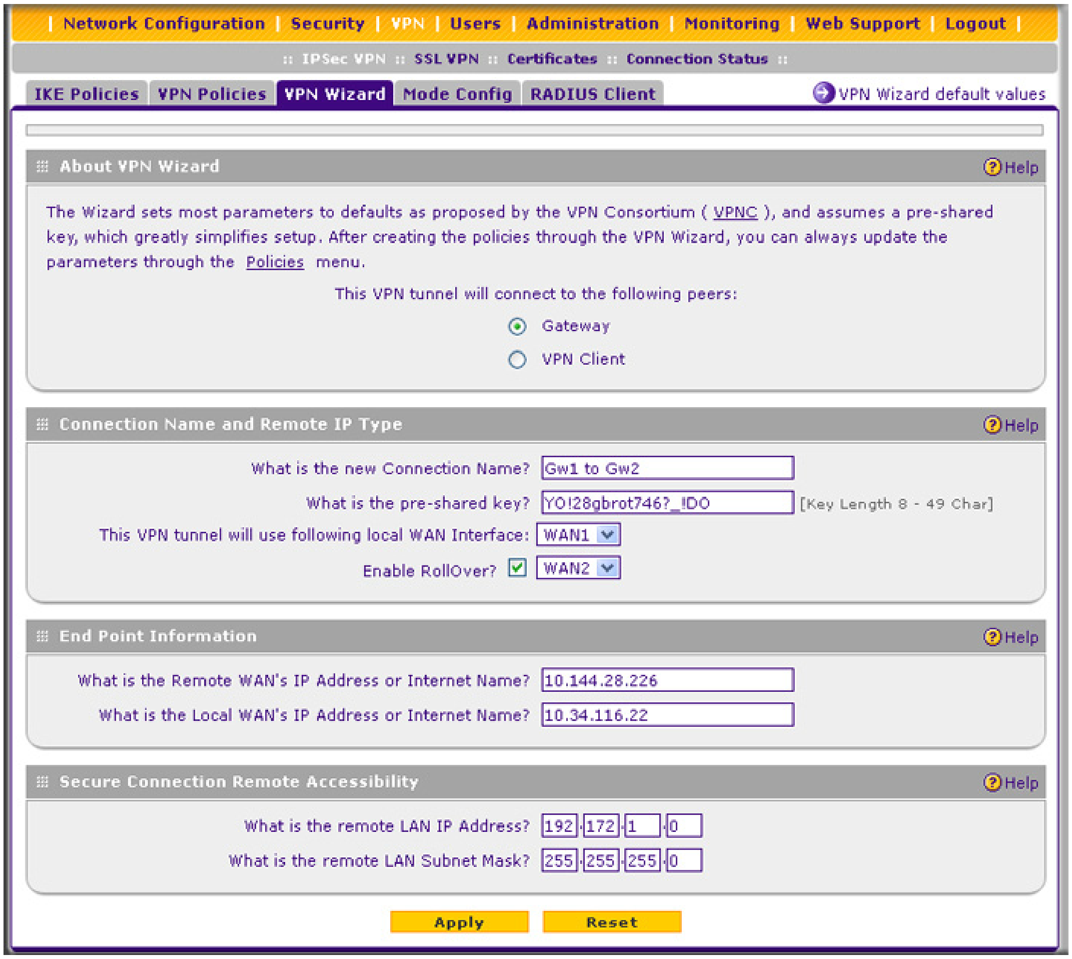

Gateway-to-Gateway Example (Single WAN Ports)
Gateway A
LAN IP
WAN IP
FQDN
INTERNET
WAN IP
Gateway B
LAN IP
VPN Router
(at office A)
Fully-Qualified Domain Names (FQDN)
- optional for Fixed IP addresses
- required for Dynamic IP addresses
VPN Router
(at office B)

Figure 76.

➤ **To set up a gateway-to-gateway VPN tunnel using the VPN Wizard.**

1. Select **VPN > IPSec VPN > VPN Wizard**. The VPN Wizard screen displays. (The following figure contains some entries as an example.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
VPN Wizard default values
Help
Apply
Reset

About VPN Wizard

The Wizard sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a pre-shared key, which greatly simplifies setup. After creating the policies through the VPN Wizard, you can always update the parameters through the Policies menu.

This VPN tunnel will connect to the following peers:

● Gateway
○ VPN Client

Connection Name and Remote IP Type

What is the new Connection Name?	Gw1 to Gw2
What is the pre-shared key?	YO!28gbrot746?_!DO [Key Length 8 - 49 Char]
This VPN tunnel will use following local WAN Interface:	WAN1
Enable RollOver? ☑	WAN2

End Point Information

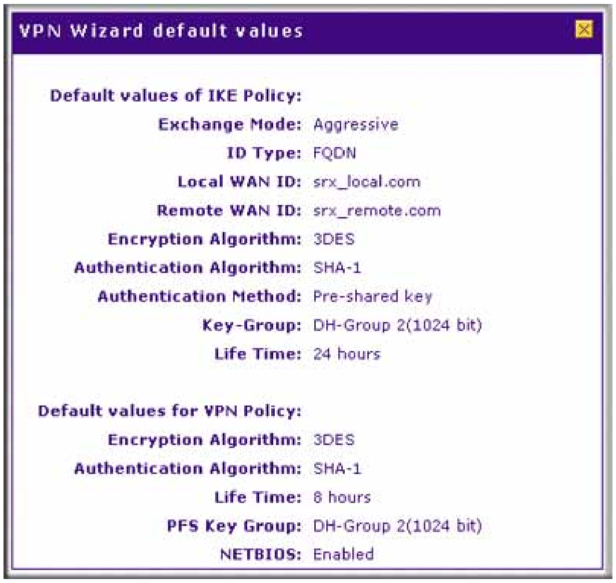
What is the Remote WAN's IP Address or Internet Name?	10.144.28.226
What is the Local WAN's IP Address or Internet Name?	10.34.116.22

Secure Connection Remote Accessibility

What is the remote LAN IP Address?	192.172.1.0
What is the remote LAN Subnet Mask?	255.255.255.0

Figure 77.

To view the wizard default settings, click the **VPN Wizard Default Values** option arrow in the upper right of the screen. A popup window appears (see *Figure 78* on page 138) displaying the wizard default values. After you have completed the wizard, you can modify these settings for the tunnel policy that you have set up.



VPN Wizard default values

Default values of IKE Policy:

Exchange Mode: Aggressive

ID Type: FQDN

Local WAN ID: srx_local.com

Remote WAN ID: srx_remote.com

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

Authentication Method: Pre-shared key

Key-Group: DH-Group 2(1024 bit)

Life Time: 24 hours

Default values for VPN Policy:

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

Life Time: 8 hours

PFS Key Group: DH-Group 2(1024 bit)

NETBIOS: Enabled

Figure 78.

2. Complete the settings as explained the following table;

Table 29. IPSec VPN Wizard settings for a gateway-to-gateway tunnel

Setting	Description
About VPN Wizard	
This VPN tunnel will connect to the following peers	Select the **Gateway** radio button. The local WAN port's IP address or Internet name appears in the End Point Information section of the screen.
Connection Name and Remote IP Type	
What is the new Connection Name?	Enter a descriptive name for the connection. This name is used to help you to manage the VPN settings; the name is not supplied to the remote VPN endpoint.
What is the pre-shared key?	Enter a pre-shared key. The key needs to be entered both here and on the remote VPN gateway. This key needs to have a minimum length of 8 characters and should not exceed 49 characters.
This VPN tunnel will use following local WAN Interface:	From the drop-down list, select one of the four WAN interfaces of the VPN firewall to specify which WAN interface the VPN tunnel uses as the local endpoint.
Enable RollOver?	If you have configured the VPN firewall to function in WAN auto-rollover mode (see *Configure the Auto-Rollover Mode and Failure Detection Method* on page 34), select the **Enable RollOver?** check box. Then, from the corresponding drop-down list, select the backup WAN interface. After an auto-rollover has occurred, the VPN tunnel will be reestablished using the backup WAN interface.

Table 29. IPSec VPN Wizard settings for a gateway-to-gateway tunnel (continued)

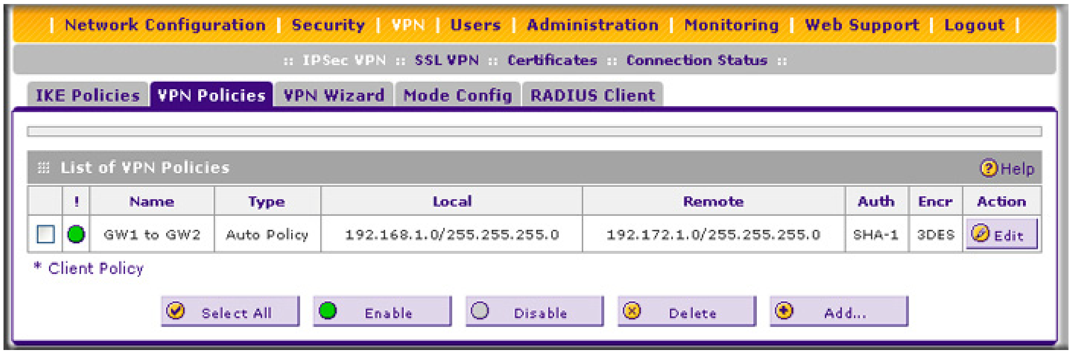
Setting	Description
End Point Information [a]	
What is the Remote WAN's IP Address or Internet Name?	Enter the IP address or Internet name (FQDN) of the WAN interface on the remote VPN tunnel endpoint.
What is the Local WAN's IP Address or Internet Name?	When you select the Gateway radio button in the About VPN Wizard section of the screen, the IP address of the VPN firewall's active WAN interface is automatically entered.
Secure Connection Remote Accessibility	
What is the remote LAN IP Address?	Enter the LAN IP address of the remote gateway. **Note:** The remote LAN IP address needs to be in a different subnet than the local LAN IP address. For example, if the local subnet is 192.168.1.x, then the remote subnet could be 192.168.10.x. but could not be 192.168.1.x. If this information is incorrect, the tunnel will fail to connect.
What is the remote LAN Subnet Mask?	Enter the LAN subnet mask of the remote gateway.

[a] *Both local and remote endpoints should be defined as either FQDNs or IP addresses. A combination of an IP address and an FQDN is not supported.*

Tip: To ensure that tunnels stay active, after completing the wizard, manually edit the VPN policy to enable keep-alive, which periodically sends ping packets to the host on the peer side of the network to keep the tunnel alive. For more information, see *Configure Keep-alives* on page 192.

Tip: For DHCP WAN configurations, first set up the tunnel with IP addresses. After you have validated the connection, you can use the wizard to create new policies using the FQDN for the WAN addresses.

3. Click **Apply** to save your settings. The IPSec VPN policy is now added to the List of VPN Policies table on the VPN Policies screen. By default, the VPN policy is enabled.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
Help
Select All
Enable
Disable
Delete
Add...

List of VPN Policies

	!	Name	Type	Local	Remote	Auth	Encr	Action
□	●	GW1 to GW2	Auto Policy	192.168.1.0/255.255.255.0	192.172.1.0/255.255.255.0	SHA-1	3DES	Edit

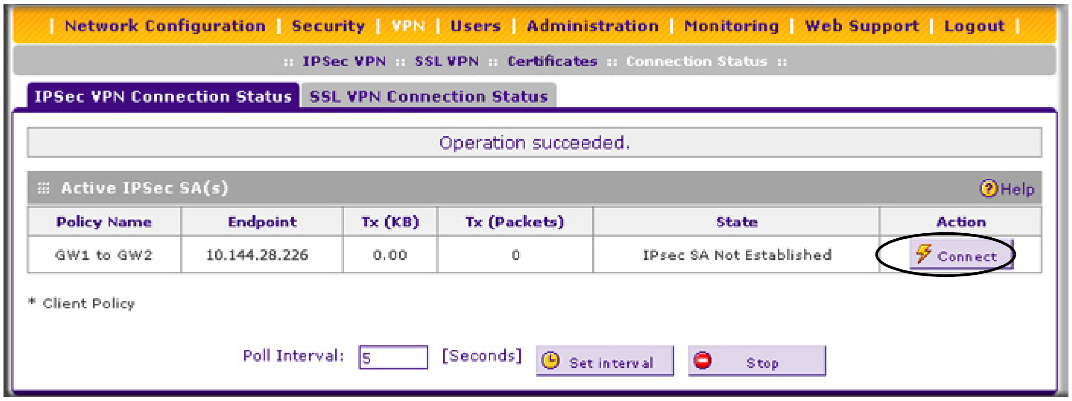
* Client Policy

Figure 79.

4. Configure a VPN policy on the remote gateway that allows connection to the VPN firewall.

5. Activate the IPSec VPN connection:

   a. Select **VPN > Connection Status**. The VPN Connection Status submenu tabs display, with the IPSec VPN Connection Status screen in view.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: Certificates :: Connection Status ::
IPSec VPN Connection Status
SSL VPN Connection Status
Help
Set interval
Stop

Operation succeeded.

Active IPSec SA(s)

Policy Name	Endpoint	Tx (KB)	Tx (Packets)	State	Action
GW1 to GW2	10.144.28.226	0.00	0	IPsec SA Not Established	Connect

* Client Policy

Poll Interval: 5 [Seconds]

Figure 80.

   b. Locate the policy in the table, and click the **Connect** table button. The IPSec VPN connection should become active.

Note: When using FQDNs, if the Dynamic DNS service is slow to update its servers when your DHCP WAN address changes, the VPN tunnel will fail because the FQDNs do not resolve to your new address. If you have the option to configure the update interval, set it to an appropriately short time.

Create a Client to Gateway VPN Tunnel

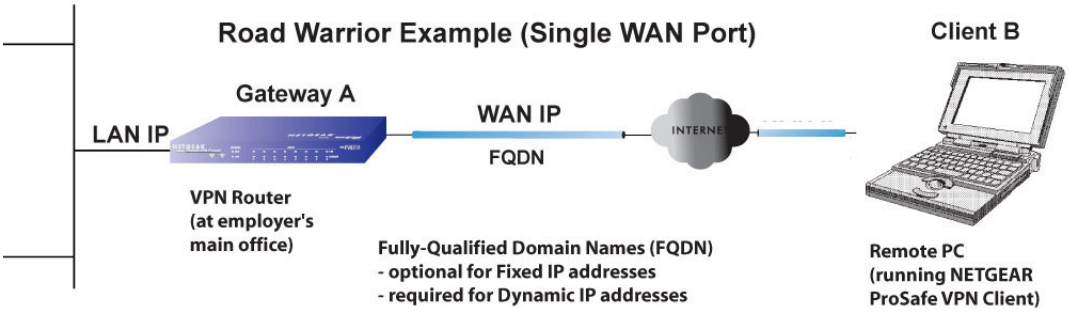

Road Warrior Example (Single WAN Port)
Client B
Gateway A
LAN IP
WAN IP
FQDN
INTERNET
VPN Router
(at employer's
main office)
Fully-Qualified Domain Names (FQDN)
- optional for Fixed IP addresses
- required for Dynamic IP addresses
Remote PC
(running NETGEAR
ProSafe VPN Client)

Figure 81.

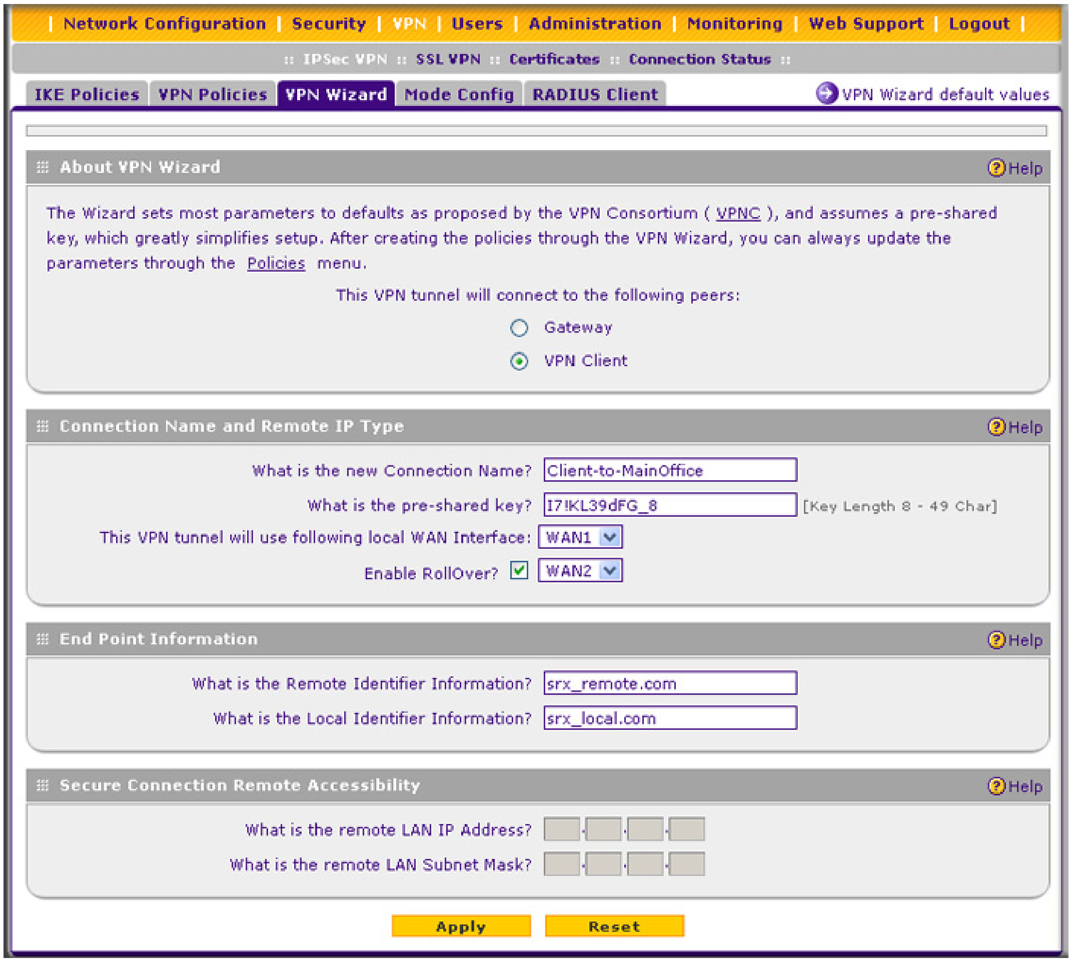
To configure a VPN client tunnel, follow the steps in the following sections:

- *Use the VPN Wizard Configure the Gateway for a Client Tunnel* on page 141
- *Use the NETGEAR VPN Client Wizard to Create a Secure Connection* on page 143 *or Manually Create a Secure Connection Using the NETGEAR VPN Client* on page 148

Use the VPN Wizard Configure the Gateway for a Client Tunnel

➢ **To set up a client-to-gateway VPN tunnel using the VPN Wizard:**

1. Select **VPN > IPSec VPN > VPN Wizard**. The VPN Wizard screen displays. (The following figure contains some entries as an example.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
VPN Wizard default values
Help
Apply
Reset

About VPN Wizard

The Wizard sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a pre-shared key, which greatly simplifies setup. After creating the policies through the VPN Wizard, you can always update the parameters through the Policies menu.

This VPN tunnel will connect to the following peers:

○ Gateway

● VPN Client

Connection Name and Remote IP Type

What is the new Connection Name? Client-to-MainOffice

What is the pre-shared key? I7!KL39dFG_8 [Key Length 8 - 49 Char]

This VPN tunnel will use following local WAN Interface: WAN1

Enable RollOver? ☑ WAN2

End Point Information

What is the Remote Identifier Information? srx_remote.com

What is the Local Identifier Information? srx_local.com

Secure Connection Remote Accessibility

What is the remote LAN IP Address? ___ . ___ . ___ . ___

What is the remote LAN Subnet Mask? ___ . ___ . ___ . ___

Figure 82.

To display the wizard default settings, click the **VPN Wizard Default Values** option arrow in the upper right of the screen. A popup window appears (see *Figure 78* on page 138), displaying the wizard default values. After you have completed the wizard, you can modify these settings for the tunnel policy that you have set up.

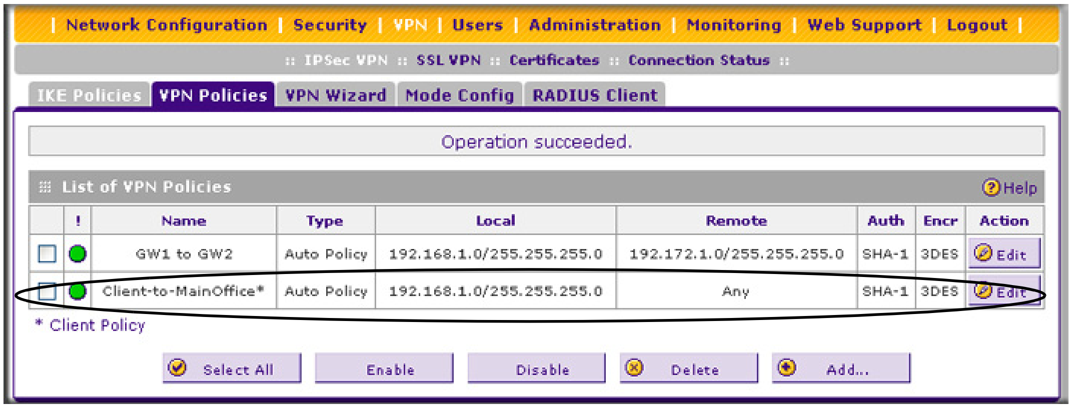
2. Complete the settings as explained the following table.

Table 30. IPSec VPN Wizard settings for a client-to-gateway tunnel

Setting	Description
About VPN Wizard	
This VPN tunnel will connect to the following peers:	Select the **VPN Client** radio button. The default remote FQDN (srx_remote.com) and the default local FQDN (srx_local.com) appear in the End Point Information section of the screen.
Connection Name and Remote IP Type	
What is the new Connection Name?	Enter a descriptive name for the connection. This name is used to help you to manage the VPN settings; the name is not supplied to the remote VPN endpoint.
What is the pre-shared key?	Enter a pre-shared key. The key needs to be entered both here and on the remote VPN gateway, or the remote VPN client. This key needs to have a minimum length of 8 characters and should not exceed 49 characters.
This VPN tunnel will use following local WAN Interface:	From the drop-down list, select one of the four WAN interfaces of the VPN firewall to specify which WAN interface the VPN tunnel uses as the local endpoint.
Enable RollOver	If you have configured the VPN firewall to function in WAN auto-rollover mode (see *Configure the Auto-Rollover Mode and Failure Detection Method* on page 34), select the **Enable RollOver** check box. Then, from the corresponding drop-down list, select the backup WAN interface. After an auto-rollover has occurred, the VPN tunnel will be reestablished using the backup WAN interface.
End Point Information [a]	
What is the Remote Identifier Information?	When you select the **Client** radio button in the About VPN Wizard section of the screen, the default remote FQDN (srx_remote.com) is automatically entered. Use the default remote FQDN or enter another FQDN.
What is the Local Identifier Information?	When you select the **Client** radio button in the About VPN Wizard section of the screen, the default local FQDN (srx_local.com) is automatically entered. Use the default local FQDN or enter another FQDN.
Secure Connection Remote Accessibility	
What is the remote LAN IP Address?	These fields are masked out for VPN client connections.
What is the remote LAN Subnet Mask?	

a. Both local and remote endpoints should be defined as either FQDNs or IP addresses. A combination of an IP address and an FQDN is not supported.

3. Click **Apply** to save your settings. The IPSec VPN policy is now added to the List of VPN Policies table on the VPN Policies screen. By default, the VPN policy is enabled.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
Help
Select All
Enable
Disable
Delete
Add...

Operation succeeded.

List of VPN Policies

	!	Name	Type	Local	Remote	Auth	Encr	Action
□	●	GW1 to GW2	Auto Policy	192.168.1.0/255.255.255.0	192.172.1.0/255.255.255.0	SHA-1	3DES	Edit
□	●	Client-to-MainOffice*	Auto Policy	192.168.1.0/255.255.255.0	Any	SHA-1	3DES	Edit

* Client Policy

Figure 83.

Note: When using FQDNs, if the dynamic DNS service is slow to update its servers when your DHCP WAN address changes, the VPN tunnel will fail because the FQDNs do not resolve to your new address. If you have the option to configure the update interval, set it to an appropriately short time.

4. Optional step: Collect the information that you need to configure the VPN client. You can print the following table to help you keep track of this information.

Table 31. Information required to configure the VPN client

Component	Example	Information to be collected
Pre-Shared Key	I7!KL39dFG_8	
Remote Identifier Information	srx_remote.com	
Local Identifier Information	srx_local.com	
Router’s LAN Network IP Address	192.168.1.0	
Router’s LAN Network Mask	255.255.255.0	
Router’s WAN IP Address	10.34.116.22	

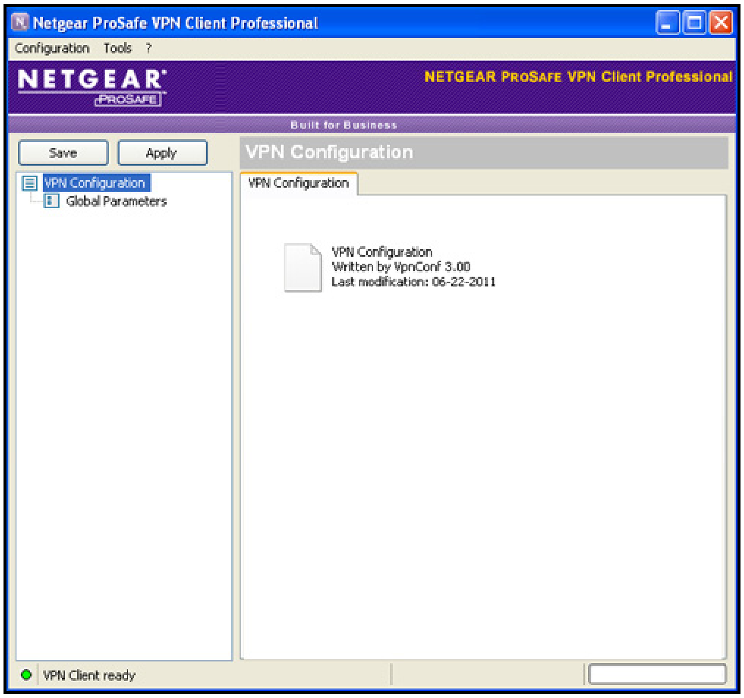
Use the NETGEAR VPN Client Wizard to Create a Secure Connection

The VPN client lets you to set up the VPN connection manually (see *Manually Create a Secure Connection Using the NETGEAR VPN Client* on page 148) or with the integrated Configuration Wizard, which is the easier and preferred method. The Configuration Wizard configures the default settings and provides basic interoperability so that the VPN client can easily communicate with the VPN firewall (or third-party VPN devices). The Configuration Wizard does not let you enter the local and remote IDs, so you need to manually enter this information.

Note: Perform these tasks from a PC that has the NETGEAR ProSafe VPN Client installed.

➢ **To use the Configuration Wizard to set up a VPN connection between the VPN client and the VPN firewall:**

1. Right-click the VPN client icon in your Windows system tray, and select **Configuration Panel**. The Configuration Panel screen displays.

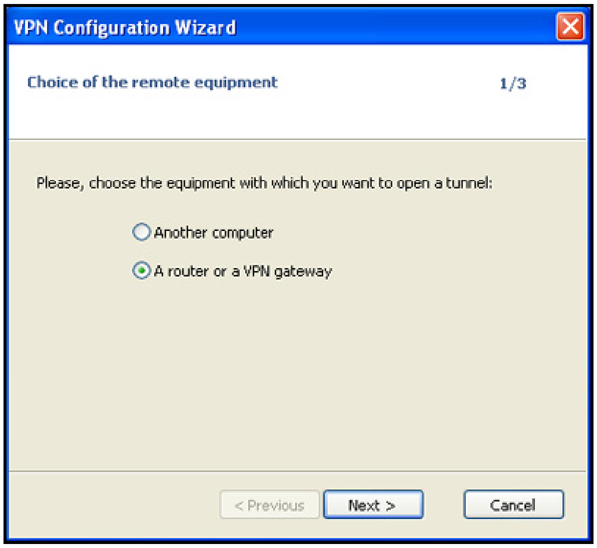


VPN Configuration
Written by VpnConf 3.00
Last modification: 06-22-2011

VPN Client ready

Figure 84.

1. From the main menu on the Configuration Panel screen, select **Configuration > Wizard**. The Choice of the remote equipment wizard screen (screen 1 of 3) displays.



VPN Configuration Wizard

Choice of the remote equipment 1/3

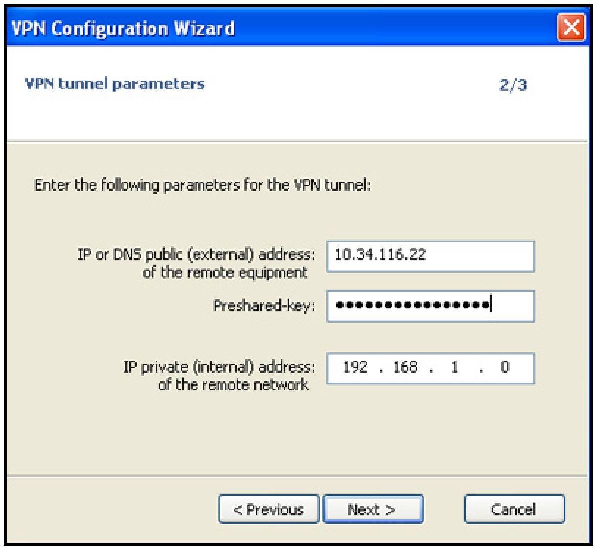
Please, choose the equipment with which you want to open a tunnel:

○ Another computer

● A router or a VPN gateway

Figure 85.

2. Select the **A router or a VPN gateway** radio button, and click **Next**. The VPN tunnel parameters wizard screen (screen 2 of 3) displays.



VPN Configuration Wizard

VPN tunnel parameters 2/3

Enter the following parameters for the VPN tunnel:

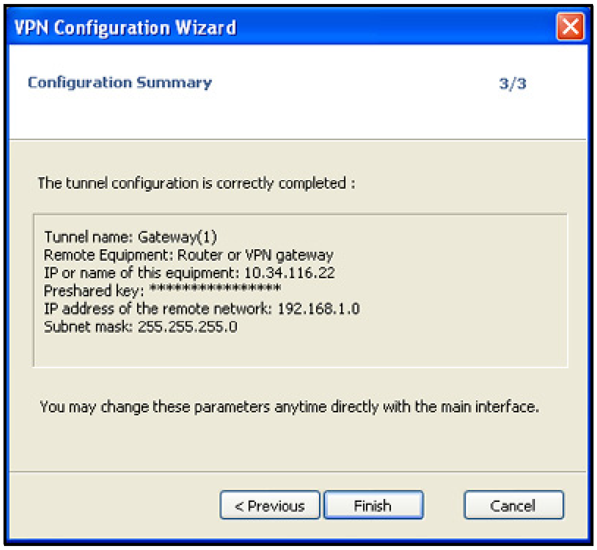
IP or DNS public (external) address: of the remote equipment: 10.34.116.22

Preshared-key: ●●●●●●●●●●●●●●●●

IP private (internal) address: of the remote network: 192 . 168 . 1 . 0

Figure 86.

3. Specify the following VPN tunnel parameters:
   - **IP or DNS public (external) address of the remote equipment**. Enter the remote IP address or DNS name of the VPN firewall. For example, enter **10.34.116.22**.
   - **Preshared key**. Enter the pre-shared key that you already specified on the VPN firewall. For example, enter **I7!KL39dFG_8**.
   - **IP private (internal) address of the remote network**. Enter the remote private IP address of the VPN firewall. For example, enter **192.168.1.0**. This IP address enables communication with the entire 192.168.1.x subnet.
4. Click **Next**. The Configuration Summary wizard screen (screen 3 of 3) displays.



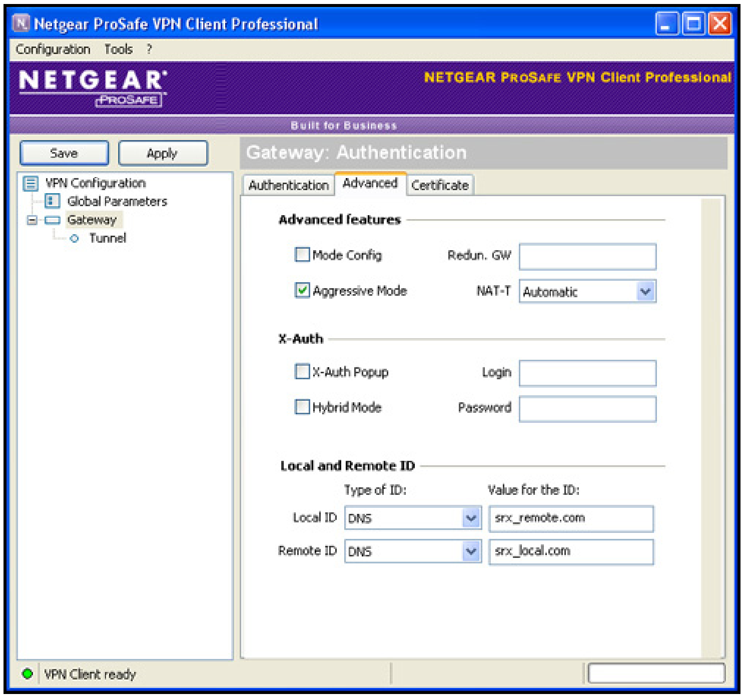
The tunnel configuration is correctly completed :

Tunnel name: Gateway(1)
Remote Equipment: Router or VPN gateway
IP or name of this equipment: 10.34.116.22
Preshared key: ****************
IP address of the remote network: 192.168.1.0
Subnet mask: 255.255.255.0

You may change these parameters anytime directly with the main interface.

Figure 87.

5. This screen is a summary screen of the new VPN configuration. Click **Finish**.
6. Specify the local and remote IDs:
   - **a.** In the tree list pane of the Configuration Panel screen, click **Gateway** (the default name given to the authentication phase). The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default.
   - **b.** Click the **Advanced** tab in the Authentication pane. The Advanced pane displays.



□ Mode Config Redun. GW

☑ Aggressive Mode NAT-T Automatic

□ X-Auth Popup Login

□ Hybrid Mode Password

Local ID DNS srx_remote.com

Remote ID DNS srx_local.com

Figure 88.

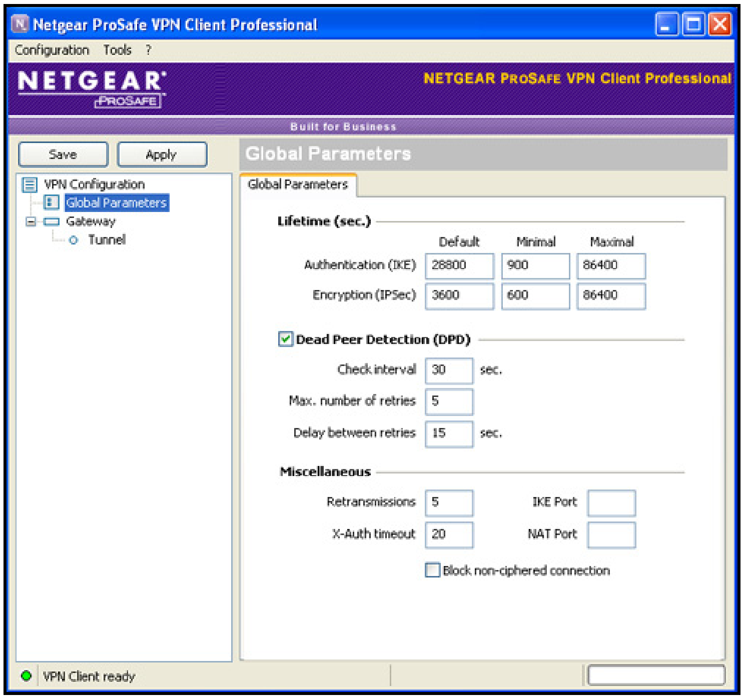
c. Specify the settings that are explained in the following table.

Table 32. VPN client advanced authentication settings

Setting	Description
Advanced features	
Aggressive Mode	Select this check box to enable aggressive mode as the negotiation mode with the VPN firewall.
NAT-T	Select **Automatic** from the drop-down list to enable the VPN client and VPN firewall to negotiate NAT-T.
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the Local ID drop-down list because you specified FQDN in the VPN firewall configuration. As the value of the ID, enter **srx_remote.com** as the local ID for the VPN client. **Note:** The remote ID on the VPN firewall is the local ID on the VPN client. It might be less confusing to configure an FQDN such as client.com as the remote ID on the VPN firewall and then enter client.com as the local ID on the VPN client.
Remote ID	As the type of ID, select **DNS** from the Remote ID drop-down list because you specified an FQDN in the VPN firewall configuration. As the value of the ID, enter **srx_local.com** as the remote ID for the VPN firewall. **Note:** The local ID on the VPN firewall is the remote ID on the VPN client. It might be less confusing to configure an FQDN such as router.com as the local ID on the VPN firewall and then enter router.com as the remote ID on the VPN client.

7. Configure the global parameters:

a. Click **Global Parameters** in the left column of the Configuration Panel screen. The Global Parameters pane displays in the Configuration Panel screen.



Global Parameters

Lifetime (sec.)

	Default	Minimal	Maximal
Authentication (IKE)	28800	900	86400
Encryption (IPSec)	3600	600	86400

☑ Dead Peer Detection (DPD)

Check interval 30 sec.

Max. number of retries 5

Delay between retries 15 sec.

Miscellaneous

Retransmissions 5 IKE Port

X-Auth timeout 20 NAT Port

□ Block non-ciphered connection

● VPN Client ready

Figure 89.

b. Specify the default lifetimes in seconds:

- **Authentication (IKE)**, **Default**. The default lifetime value is 3600 seconds. Change this setting to **28800** seconds to match the configuration of the VPN firewall.
- **Encryption (IPSec)**, **Default**. The default lifetime value is 1200 seconds. Change this setting to **3600** seconds to match the configuration of the VPN firewall.

8. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

The VPN client configuration is now complete.

Instead of using the wizard on the VPN client, you can also manually configure the VPN client, which is explained in the following section.

Manually Create a Secure Connection Using the NETGEAR VPN Client

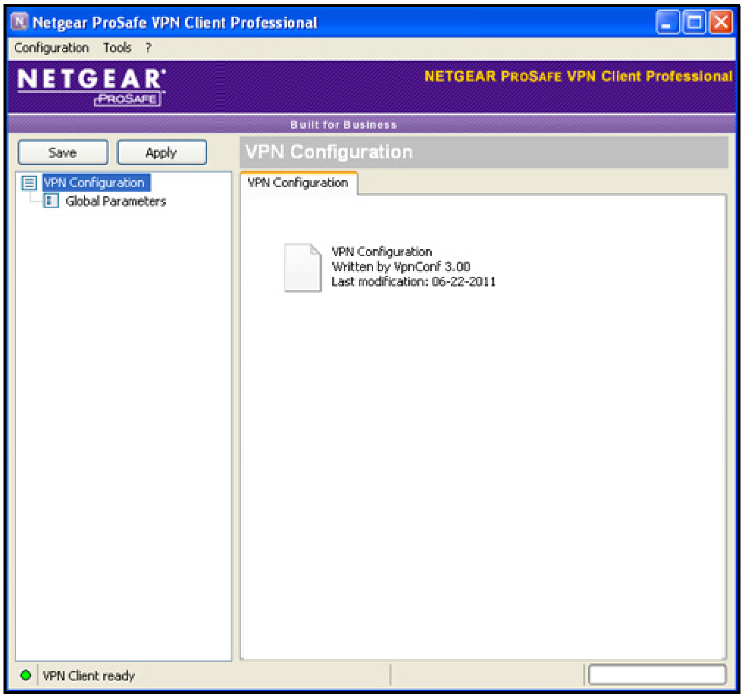
Note: Perform these tasks from a PC that has the NETGEAR ProSafe VPN Client installed.

To manually configure a VPN connection between the VPN client and the VPN firewall, create authentication settings (phase 1 settings), create an associated IPSec configuration (phase 2 settings), and then specify the global parameters.

Configure the Authentication Settings (Phase 1 Settings)

➤ **To create new authentication settings:**

1. Right-click the VPN client icon in your Windows system tray, and select **Configuration Panel**. The Configuration Panel screen displays.



VPN Configuration
Written by VpnConf 3.00
Last modification: 06-22-2011

Figure 90.

2. In the tree list pane of the Configuration Panel screen, right-click **VPN Configuration** and select **New Phase 1**.

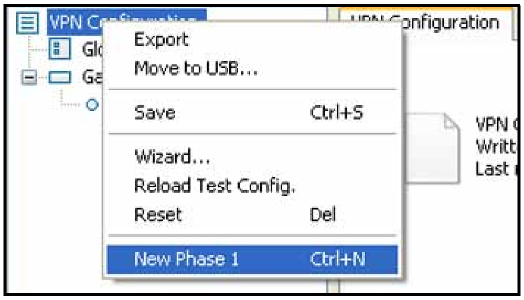
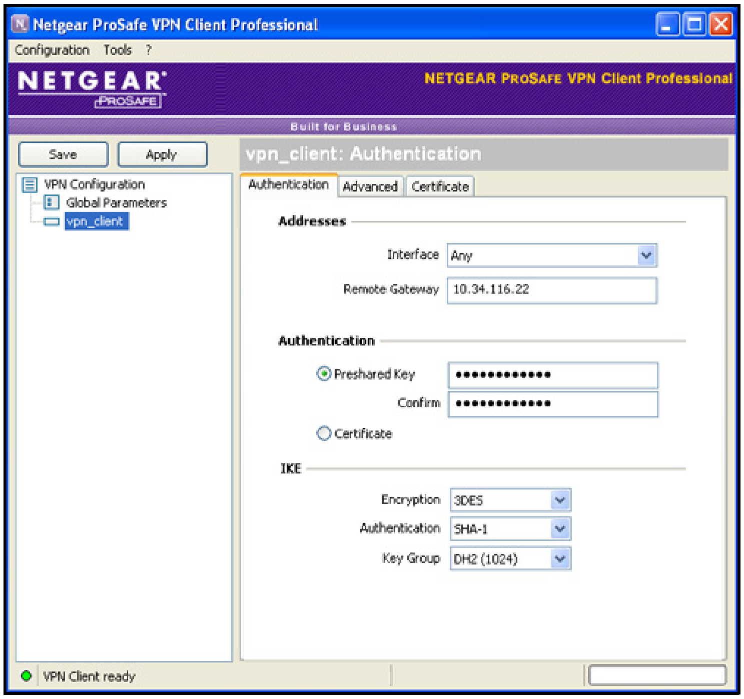


Figure 91.

3. Change the name of the authentication phase (the default is Gateway):
   - **a.** Right-click the authentication phase name.
   - **b.** Select **Rename**.
   - **c.** Type **vpn_client**.
   - **d.** Click anywhere in the tree list pane.

> **Note:** *This is the name for the authentication phase that is used only for the VPN client, not during IKE negotiation. You can view and change this name in the tree list pane. This name needs to be a unique name.*

The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default.



vpn_client: Authentication

Addresses

Interface: Any

Remote Gateway: 10.34.116.22

Authentication

● Preshared Key: •••••••••••••

Confirm: •••••••••••••

○ Certificate

IKE

Encryption: 3DES

Authentication: SHA-1

Key Group: DH2 (1024)

VPN Client ready

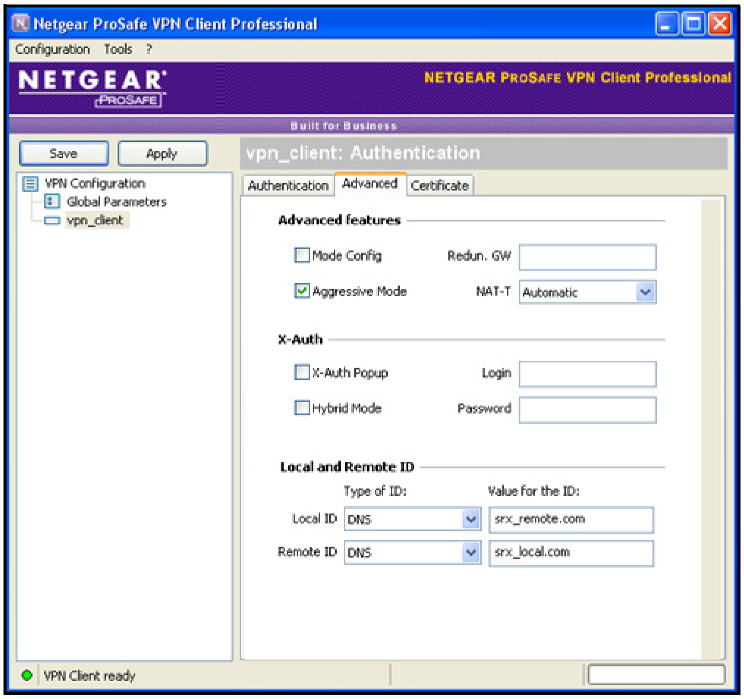
Figure 92.

4. Specify the settings that are explained in the following table.

Table 33. VPN client authentication settings

Setting	Description	
Interface	Select **Any** from the drop-down list.	
Remote Gateway	Enter the remote IP address or DNS name of the VPN firewall. For example, enter **10.34.116.22**.	
Preshared Key	Select the **Preshared Key** radio button. Enter the pre-shared key that you already specified on the VPN firewall. For example, enter **I7!KL39dFG_8**. Confirm the key in the Confirm field.	
IKE	Encryption	Select the **3DES** encryption algorithm from the drop-down list.
	Authentication	Select the **SHA1** authentication algorithm from the drop-down list.
	Key Group	Select the **DH2 (1024)** key group from the drop-down list. **Note:** On the VPN firewall, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).

5. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.
6. Click the **Advanced** tab in the Authentication pane. The Advanced pane displays.



Advanced features

☐ Mode Config   Redun. GW

☑ Aggressive Mode   NAT-T Automatic

X-Auth

☐ X-Auth Popup   Login

☐ Hybrid Mode   Password

Local and Remote ID

	Type of ID:	Value for the ID:
Local ID	DNS	srx_remote.com
Remote ID	DNS	srx_local.com

Figure 93.

7. Specify the settings that are explained in the following table.

Table 34. VPN client advanced authentication settings

Setting	Description
Advanced features	
Aggressive Mode	Select this check box to enable aggressive mode as the negotiation mode with the VPN firewall.
NAT-T	Select **Automatic** from the drop-down list to enable the VPN client and VPN firewall to negotiate NAT-T.

Table 34. VPN client advanced authentication settings (continued)

Setting	Description
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the Local ID drop-down list because you specified FQDN in the VPN firewall configuration. As the value of the ID, enter **srx_remote.com** as the local ID for the VPN client. **Note:** The remote ID on the VPN firewall is the local ID on the VPN client. It might be less confusing to configure an FQDN such as client.com as the remote ID on the VPN firewall and then enter client.com as the local ID on the VPN client.
Remote ID	As the type of ID, select **DNS** from the Remote ID drop-down list because you specified an FQDN in the VPN firewall configuration. As the value of the ID, enter **srx_local.com** as the remote ID for the VPN firewall. **Note:** The local ID on the VPN firewall is the remote ID on the VPN client. It might be less confusing to configure an FQDN such as router.com as the local ID on the VPN firewall and then enter router.com as the remote ID on the VPN client.

8. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Create the IPSec Configuration (Phase 2 Settings)

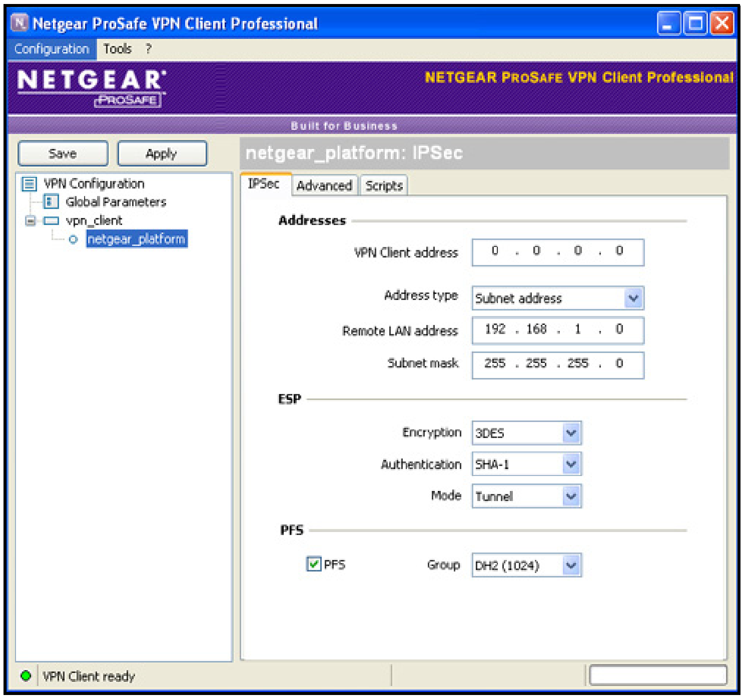
Note: On the VPN firewall, the IPSec configuration (phase 2 settings) is referred to as the IKE settings.

➤ **To create an IPSec configuration:**

1. In the tree list pane of the Configuration Panel screen, right-click the **vpn_client** authentication phase name, and then select **New Phase 2**.
2. Change the name of the IPSec configuration (the default is Tunnel):
   a. Right-click the IPSec configuration name.
   b. Select **Rename**.
   c. Type **netgear_platform**.
   d. Click anywhere in the tree list pane.

   Note: *This is the name for the IPSec configuration that is used only for the VPN client, not during IPSec negotiation. You can view and change this name in the tree list pane. This name needs to be a unique name.*

   The IPSec pane displays in the Configuration Panel screen, with the IPSec tab selected by default.



netgear_platform: IPSec

Addresses

VPN Client address 0 . 0 . 0 . 0

Address type Subnet address

Remote LAN address 192 . 168 . 1 . 0

Subnet mask 255 . 255 . 255 . 0

ESP

Encryption 3DES

Authentication SHA-1

Mode Tunnel

PFS

☑ PFS Group DH2 (1024)

VPN Client ready

Figure 94.

3. Specify the settings that are explained in the following table.

Table 35. VPN client IPSec configuration settings

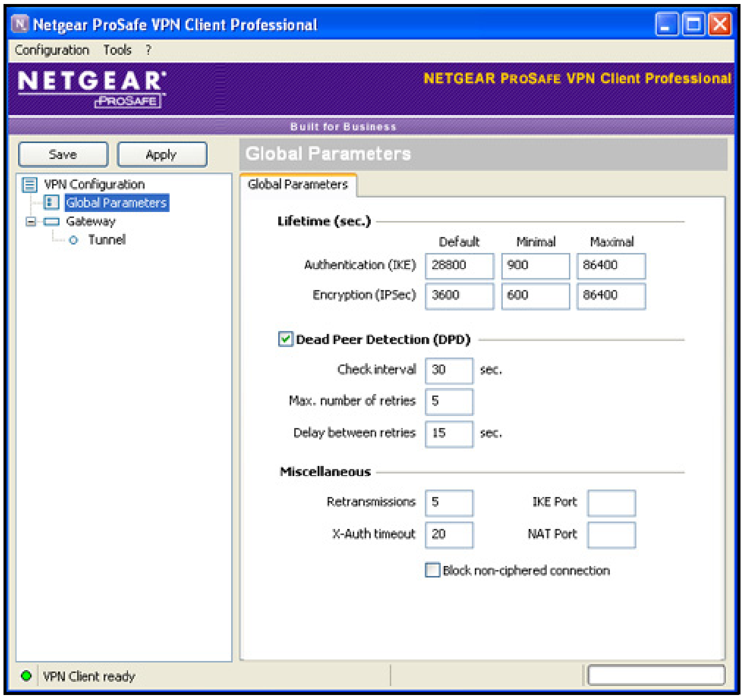
Setting	Description	
VPN Client address	Either enter **0.0.0.0** as the IP address, or enter a virtual IP address that is used by the VPN client in the VPN firewall's LAN; the computer (for which the VPN client opened a tunnel) appears in the LAN with this IP address.	
Address Type	Select **Subnet address** from the drop-down list. This selection defines which addresses the VPN client can communicate with after the VPN tunnel is established.	
Remote LAN address	Enter **192.168.1.0** as the remote IP address (that is, LAN network address) of the gateway that opens the VPN tunnel.	
Subnet Mask	Enter **255.255.255.0** as the remote subnet mask of the gateway that opens the VPN tunnel.	
ESP	Encryption	Select **3DES** as the encryption algorithm from the drop-down list.
	Authentication	Select **SHA-1** as the authentication algorithm from the drop-down list.
	Mode	Select **Tunnel** as the encapsulation mode from the drop-down list.
PFS and Group	Select the **PFS** check box, and then select the **DH2 (1024)** key group from the drop-down list. **Note:** On the VPN firewall, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).	

4. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Configure the Global Parameters

➤ **To specify the global parameters:**

1. Click **Global Parameters** in the left column of the Configuration Panel screen. The Global Parameters pane displays in the Configuration Panel screen.



Lifetime (sec.)

	Default	Minimal	Maximal
Authentication (IKE)	28800	900	86400
Encryption (IPSec)	3600	600	86400

☑ **Dead Peer Detection (DPD)**

Check interval 30 sec.

Max. number of retries 5

Delay between retries 15 sec.

Miscellaneous

Retransmissions 5 IKE Port

X-Auth timeout 20 NAT Port

☐ Block non-ciphered connection

Figure 95.

2. Specify the default lifetimes in seconds:
   - **Authentication (IKE)**, **Default**. The default lifetime value is 3600 seconds. Change this setting to **28800** seconds to match the configuration of the VPN firewall.
   - **Encryption (IPSec)**, **Default**. The default lifetime value is 1200 seconds. Change this setting to **3600** seconds to match the configuration of the VPN firewall.
3. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

The VPN firewall configuration is now complete.

Test the Connection and View Connection and Status Information

Both the NETGEAR ProSafe VPN Client and the VPN firewall provide VPN connection and status information. This information is useful for verifying the status of a connection and troubleshooting problems with a connection.

Test the NETGEAR VPN Client Connection

There are many ways to establish a connection. The following procedures assume that you use the default authentication phase name *Gateway* and the default IPSec configuration name *Tunnel*. If you manually set up the connection and changed the names, use *vpn_client* (or any other name that you have configured) as the authentication phase name and *netgear_platform* (or any other name that you have configured) as the IPSec configuration name.

➤ **To establish a connection, use one of the following three methods:**

- **Use the Configuration Panel screen**. In the tree list pane of the Configuration Panel screen, perform *one* of the following tasks:
  - Click the **Tunnel** IPSec configuration name, and press **Ctrl+O.**
  - Right-click the **Tunnel** IPSec configuration name, and select **Open tunnel**.

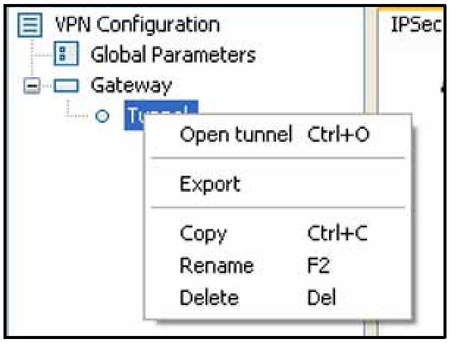


Figure 96.

- **Use the Connection Panel screen**. On the main menu of the Configuration Panel screen, select **Tools > Connection Panel** to open the Connection Panel screen.

  Perform *one* of the following tasks:

  - Double-click **Gateway-Tunnel**.
  - Right-click **Gateway-Tunnel**, and click **Open tunnel**.
  - Click **Gateway-Tunnel**, and press **Ctrl+O**.

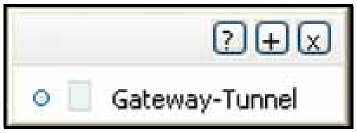


Figure 97.

- **Use the system-tray icon**. Right-click the system tray icon, and click **Open tunnel ‘Tunnel’**.

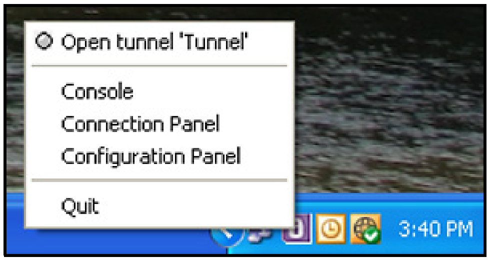


Figure 98.

Whichever way you choose to open the tunnel, when the tunnel opens successfully, the *Tunnel opened* message displays above the system tray:

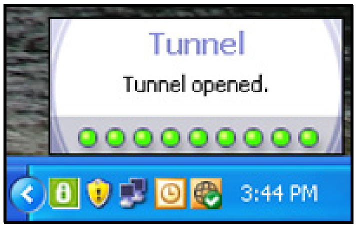
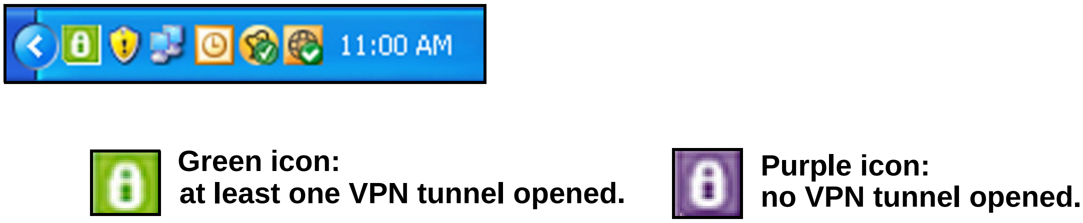


Figure 99.

Once launched, the VPN client displays an icon in the system tray that indicates whether or not a tunnel is opened, using a color code:



Green icon:
at least one VPN tunnel opened.

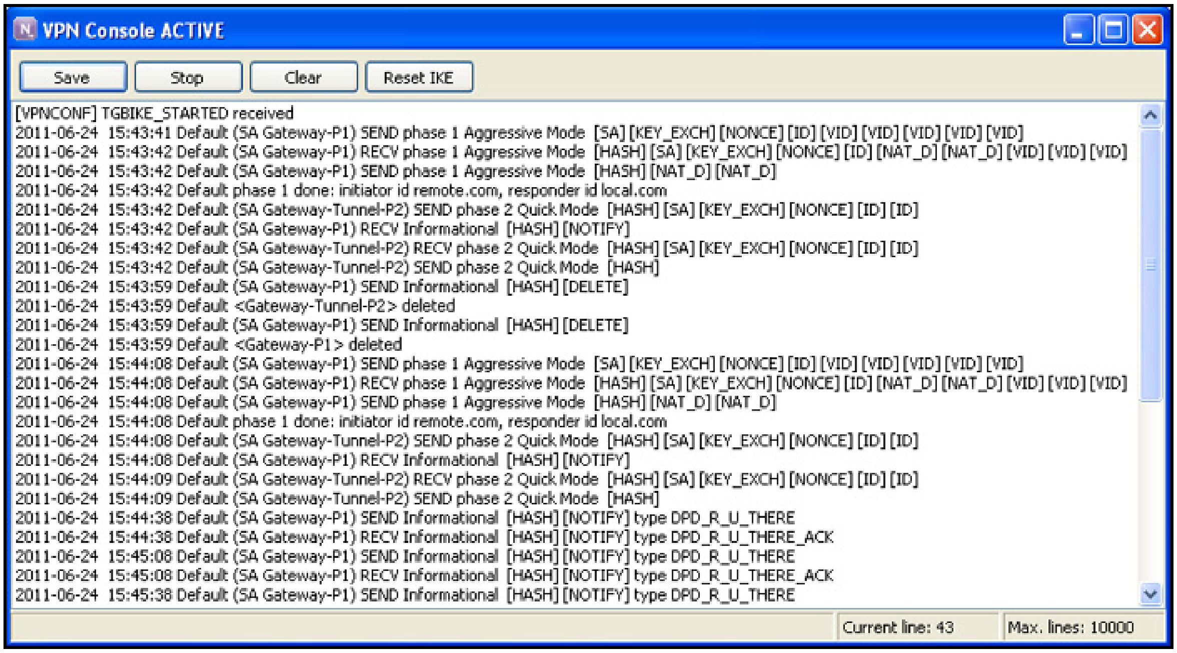
Purple icon:
no VPN tunnel opened.

Figure 100.

NETGEAR VPN Client Status and Log Information

➢ **To view detailed negotiation and error information on the NETGEAR VPN client:**

Right-click the VPN client icon in the system tray, and select **Console**. The VPN Client Console Active screen displays.



```
[VPNCONF] TGBIKE_STARTED received
2011-06-24  15:43:41 Default (SA Gateway-P1) SEND phase 1 Aggressive Mode  [SA] [KEY_EXCH] [NONCE] [ID] [VID] [VID] [VID] [VID] [VID]
2011-06-24  15:43:42 Default (SA Gateway-P1) RECV phase 1 Aggressive Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [NAT_D] [NAT_D] [VID] [VID] [VID]
2011-06-24  15:43:42 Default (SA Gateway-P1) SEND phase 1 Aggressive Mode  [HASH] [NAT_D] [NAT_D]
2011-06-24  15:43:42 Default phase 1 done: initiator id remote.com, responder id local.com
2011-06-24  15:43:42 Default (SA Gateway-Tunnel-P2) SEND phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
2011-06-24  15:43:42 Default (SA Gateway-P1) RECV Informational  [HASH] [NOTIFY]
2011-06-24  15:43:42 Default (SA Gateway-Tunnel-P2) RECV phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
2011-06-24  15:43:42 Default (SA Gateway-Tunnel-P2) SEND phase 2 Quick Mode  [HASH]
2011-06-24  15:43:59 Default (SA Gateway-P1) SEND Informational  [HASH] [DELETE]
2011-06-24  15:43:59 Default <Gateway-Tunnel-P2> deleted
2011-06-24  15:43:59 Default (SA Gateway-P1) SEND Informational  [HASH] [DELETE]
2011-06-24  15:43:59 Default <Gateway-P1> deleted
2011-06-24  15:44:08 Default (SA Gateway-P1) SEND phase 1 Aggressive Mode  [SA] [KEY_EXCH] [NONCE] [ID] [VID] [VID] [VID] [VID] [VID]
2011-06-24  15:44:08 Default (SA Gateway-P1) RECV phase 1 Aggressive Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [NAT_D] [NAT_D] [VID] [VID] [VID]
2011-06-24  15:44:08 Default (SA Gateway-P1) SEND phase 1 Aggressive Mode  [HASH] [NAT_D] [NAT_D]
2011-06-24  15:44:08 Default phase 1 done: initiator id remote.com, responder id local.com
2011-06-24  15:44:08 Default (SA Gateway-Tunnel-P2) SEND phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
2011-06-24  15:44:08 Default (SA Gateway-P1) RECV Informational  [HASH] [NOTIFY]
2011-06-24  15:44:09 Default (SA Gateway-Tunnel-P2) RECV phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
2011-06-24  15:44:09 Default (SA Gateway-Tunnel-P2) SEND phase 2 Quick Mode  [HASH]
2011-06-24  15:44:38 Default (SA Gateway-P1) SEND Informational  [HASH] [NOTIFY] type DPD_R_U_THERE
2011-06-24  15:44:38 Default (SA Gateway-P1) RECV Informational  [HASH] [NOTIFY] type DPD_R_U_THERE_ACK
2011-06-24  15:45:08 Default (SA Gateway-P1) SEND Informational  [HASH] [NOTIFY] type DPD_R_U_THERE
2011-06-24  15:45:08 Default (SA Gateway-P1) RECV Informational  [HASH] [NOTIFY] type DPD_R_U_THERE_ACK
2011-06-24  15:45:38 Default (SA Gateway-P1) SEND Informational  [HASH] [NOTIFY] type DPD_R_U_THERE
```

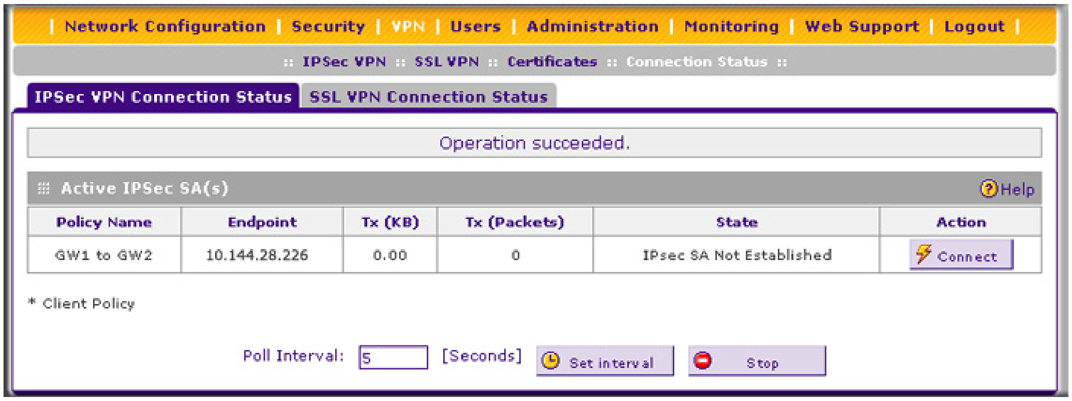
Current line: 43 | Max. lines: 10000

Figure 101.

View the VPN Firewall IPSec VPN Connection Status

➤ To review the status of current IPSec VPN tunnels:

Select **VPN > Connection Status**. The VPN Connection Status submenu tabs display, with the IPSec VPN Connection Status screen in view. (The following figure shows an IPSec SA as an example.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: Certificates :: Connection Status ::
IPSec VPN Connection Status
SSL VPN Connection Status
Help
Set interval
Stop

Operation succeeded.

Active IPSec SA(s)

Policy Name	Endpoint	Tx (KB)	Tx (Packets)	State	Action
GW1 to GW2	10.144.28.226	0.00	0	IPsec SA Not Established	Connect

* Client Policy

Poll Interval: 5 [Seconds]

Figure 102.

The Active IPSec SAs table lists each active connection with the information that is described in the following table. The default poll interval is 5 seconds. To change the poll interval period, enter a new value in the Poll Interval field, and then click **Set Interval**. To stop polling, click **Stop**.

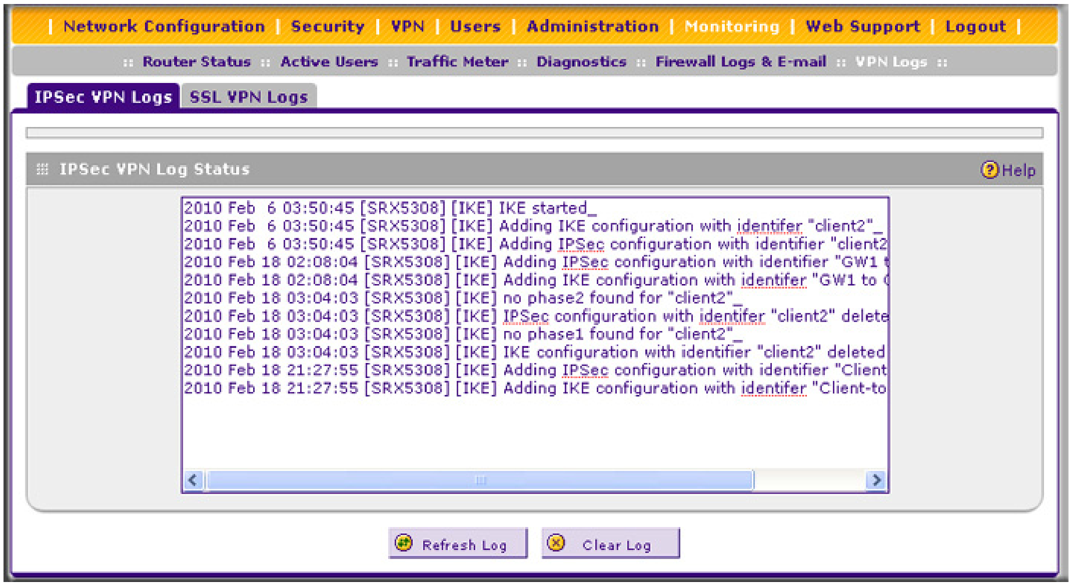
Table 36. IPSec VPN Connection Status screen information

Item	Description
Policy Name	The name of the VPN policy that is associated with this SA.
Endpoint	The IP address on the remote VPN endpoint.
Tx (KB)	The amount of data that is transmitted over this SA.
Tx (Packets)	The number of IP packets that are transmitted over this SA.
State	The current status of the SA. Phase 1 is the authentication phase and Phase 2 is key exchange phase. If there is no connection, the status is IPSec SA Not Established.
Action	Click the **Connect** table button to build the connection, or click the **Disconnect** table button to terminate the connection.

View the VPN Firewall IPSec VPN Logs

➤ **To view the IPSec VPN logs:**

Select **Monitoring > VPN Logs**. The VPN Logs submenu tabs display, with the IPSec VPN Logs screen in view.:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
IPSec VPN Logs
SSL VPN Logs
IPSec VPN Log Status
Help
Refresh Log
Clear Log

```
2010 Feb  6 03:50:45 [SRX5308] [IKE] IKE started_
2010 Feb  6 03:50:45 [SRX5308] [IKE] Adding IKE configuration with identifer "client2"_
2010 Feb  6 03:50:45 [SRX5308] [IKE] Adding IPSec configuration with identifier "client2
2010 Feb 18 02:08:04 [SRX5308] [IKE] Adding IPSec configuration with identifier "GW1 t
2010 Feb 18 02:08:04 [SRX5308] [IKE] Adding IKE configuration with identifer "GW1 to
2010 Feb 18 03:04:03 [SRX5308] [IKE] no phase2 found for "client2"_
2010 Feb 18 03:04:03 [SRX5308] [IKE] IPSec configuration with identifer "client2" delete
2010 Feb 18 03:04:03 [SRX5308] [IKE] no phase1 found for "client2"_
2010 Feb 18 03:04:03 [SRX5308] [IKE] IKE configuration with identifier "client2" deleted
2010 Feb 18 21:27:55 [SRX5308] [IKE] Adding IPSec configuration with identifier "Client
2010 Feb 18 21:27:55 [SRX5308] [IKE] Adding IKE configuration with identifer "Client-to
```

Figure 103.

Click **Refresh Log** to view the most recent entries. Click **Clear Log** to remove all entries.

Manage IPSec VPN Policies

After you have used the VPN Wizard to set up a VPN tunnel, a VPN policy and an IKE policy are stored in separate policy tables. The name that you selected as the VPN tunnel connection name during the VPN Wizard setup identifies both the VPN policy and IKE policy. You can edit existing policies, or manually add new VPN and IKE policies directly in the policy tables.

Configure IKE Policies

The Internet Key Exchange (IKE) protocol performs negotiations between the two VPN gateways, and provides automatic management of the keys that are used for IPSec connections. It is important to remember that:

- An automatically generated VPN policy (Auto Policy) needs to use the IKE negotiation protocol.
- A manually generated VPN policy (Manual Policy) cannot use the IKE negotiation protocol.

IKE policies are activated when the following situations occur:

1. The VPN policy selector determines that some traffic matches an existing VPN policy:
   - If the VPN policy is of an Auto Policy type, the IKE policy that is specified in the Auto Policy Parameters section of the Add VPN Policy screen (see *Figure 107* on page 168) is used to start negotiations with the remote VPN gateway.
   - If the VPN policy is of a Manual Policy type, the settings that are specified in the Manual Policy Parameters section of the Add VPN Policy screen (see *Figure 107* on page 168) are accessed, and the first matching IKE policy is used to start negotiations with the remote VPN gateway:
     - If negotiations fail, the next matching IKE policy is used.
     - If none of the matching IKE policies are acceptable to the remote VPN gateway, then a VPN tunnel cannot be established.
2. An IKE session is established, using the security association (SA) settings that are specified in a matching IKE policy:
   - Keys and other settings are exchanged.
   - An IPSec SA is established, using the settings that are specified in the VPN policy.

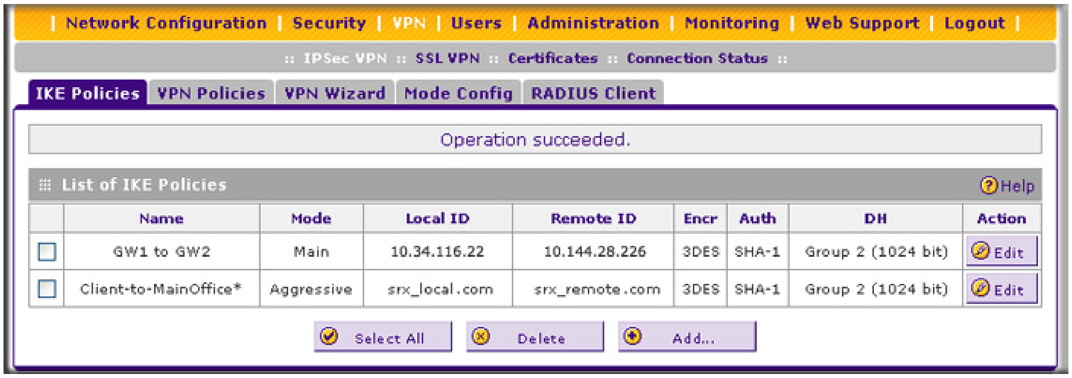
The VPN tunnel is then available for data transfer.

When you use the VPN Wizard to set up a VPN tunnel, an IKE policy is established and populated in the List of IKE Policies, and is given the same name as the new VPN connection name. You can also edit exiting policies or add new IKE policies from the IKE Policies screen.

IKE Policies Screen

➢ To access the IKE Policies screen:

Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display, with the IKE Policies screen in view (The following figure shows some examples).


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
Help
Select All
Delete
Add...

Operation succeeded.

List of IKE Policies

	Name	Mode	Local ID	Remote ID	Encr	Auth	DH	Action
□	GW1 to GW2	Main	10.34.116.22	10.144.28.226	3DES	SHA-1	Group 2 (1024 bit)	Edit
□	Client-to-MainOffice*	Aggressive	srx_local.com	srx_remote.com	3DES	SHA-1	Group 2 (1024 bit)	Edit

Figure 104.

Each policy contains the data that are explained in the following table These fields are explained in more detail in *Table 38* on page 162.

Table 37. IKE Policies screen information

Item	Description
Name	The name that identifies the IKE policy. When you use the VPN Wizard to set up a VPN policy, an accompanying IKE policy is automatically created with the same name that you select for the VPN policy. **Note:** The name is not supplied to the remote VPN endpoint.
Mode	The exchange mode: Main or Aggressive.
Local ID	The IKE/ISAKMP identifier of the VPN firewall. The remote endpoint needs to have this value as its remote ID.
Remote ID	The IKE/ISAKMP identifier of the remote endpoint, which needs to have this value as its local ID.
Encr	The encryption algorithm that is used for the IKE security association (SA). This setting needs to match the setting on the remote endpoint.
Auth	The authentication algorithm that is used for the IKE SA. This setting needs to match the setting on the remote endpoint.
DH	The Diffie-Hellman (DH) group that is used when exchanging keys. This setting needs to match the setting on the remote endpoint.

➢ To delete one or more IKE polices:

1. Select the check box to the left of the policy that you want to delete, or click the **Select All** table button to select all IKE policies.

2. Click the **Delete** table button.

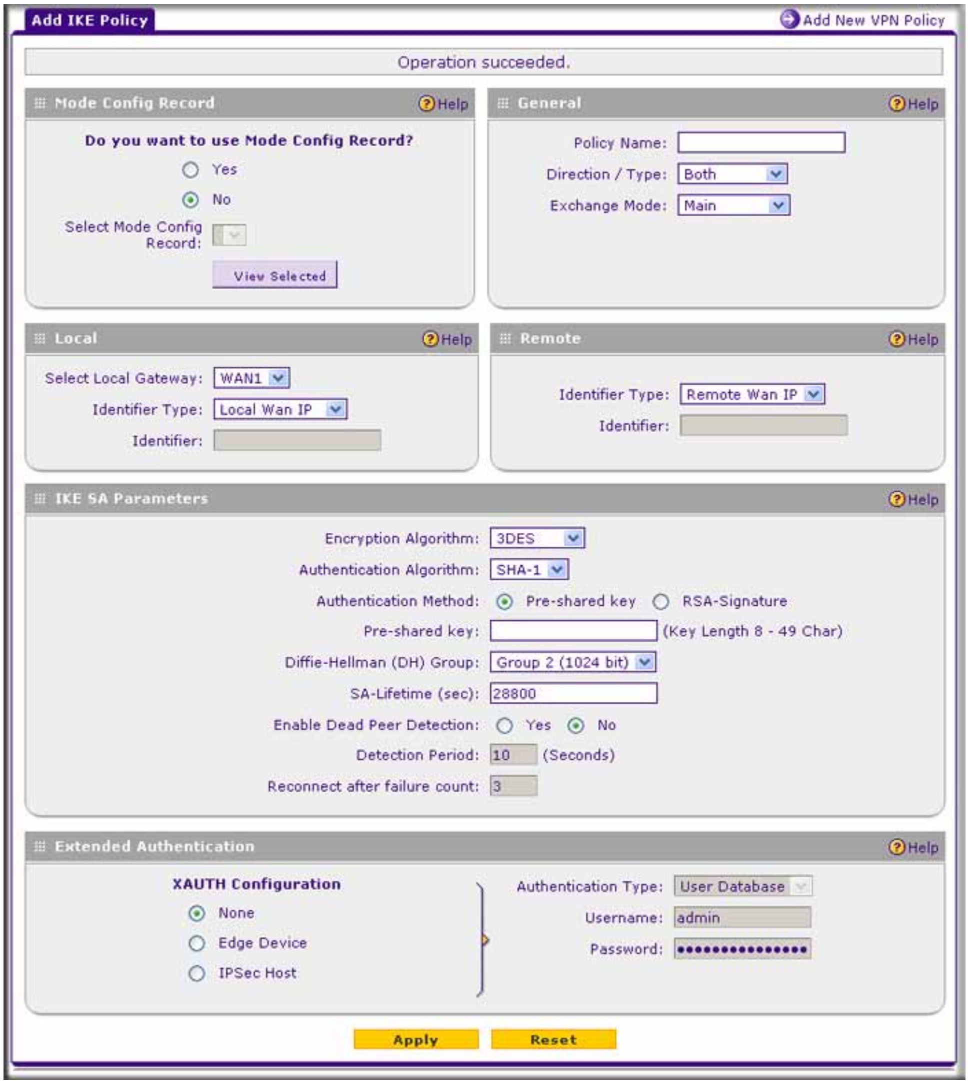
To add or edit an IKE policy, see *Manually Add or Edit an IKE Policy* on this page.

Note: You cannot delete or edit an IKE policy for which the VPN policy is active. You first need to disable or delete the VPN policy before you can delete or edit the IKE policy.

Manually Add or Edit an IKE Policy

➤ **To manually add an IKE policy:**

1. Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display, with the IKE Policies screen in view (see *Figure 104* on page 160).
2. Under the List of IKE Policies table, click the **Add** table button. The Add IKE Policy screen displays:



Operation succeeded.

Do you want to use Mode Config Record?

○ Yes
● No

Select Mode Config Record:

Policy Name:
Direction / Type: Both
Exchange Mode: Main

Select Local Gateway: WAN1
Identifier Type: Local Wan IP
Identifier:

Identifier Type: Remote Wan IP
Identifier:

Encryption Algorithm: 3DES
Authentication Algorithm: SHA-1
Authentication Method: ● Pre-shared key ○ RSA-Signature
Pre-shared key: (Key Length 8 - 49 Char)
Diffie-Hellman (DH) Group: Group 2 (1024 bit)
SA-Lifetime (sec): 28800
Enable Dead Peer Detection: ○ Yes ● No
Detection Period: 10 (Seconds)
Reconnect after failure count: 3

XAUTH Configuration
● None
○ Edge Device
○ IPSec Host

Authentication Type: User Database
Username: admin
Password: •••••••••••••••

Figure 105.

3. Complete the settings as explained the following table.

Table 38. Add IKE Policy screen settings

<table>
<tr><th>Setting</th><th colspan="2">Description</th></tr>
<tr><td colspan="3"><b>Mode Config Record</b></td></tr>
<tr><td rowspan="2">Do you want to use Mode Config Record?</td><td colspan="2">Specify whether or not the IKE policy uses a Mode Config record. For information about how to define a Mode Config record, see <i>Mode Config Operation</i> on page 176. Select one of the following radio buttons:
• <b>Yes</b>. IP addresses are assigned to remote VPN clients. You need to select a Mode Config record from the drop-down list.
• <b>No</b>. Disables Mode Config for this IKE policy.
<b>Note:</b> Because Mode Config functions only in Aggressive mode, selecting the Yes radio button sets the tunnel exchange mode to Aggressive mode and disables the Main mode. Mode Config also requires that both the local and remote ends are defined by their FQDNs.
<b>Note:</b> An XAUTH configuration via an edge device is not possible without Mode Config and is therefore disabled too. For more information about XAUTH, see <i>Configure Extended Authentication (XAUTH)</i> on page 172.</td></tr>
<tr><td>Select Mode Config Record</td><td>From the drop-down list, select one of the Mode Config records that you defined on the Add Mode Config Record screen (see <i>Configure Mode Config Operation on the VPN Firewall</i> on page 177).
<b>Note:</b> Click the <b>View Selected</b> button to open the Selected Mode Config Record Details popup window.</td></tr>
<tr><td colspan="3"><b>General</b></td></tr>
<tr><td>Policy Name</td><td colspan="2">A descriptive name of the IKE policy for identification and management purposes.
<b>Note:</b> The name is not supplied to the remote VPN endpoint.</td></tr>
<tr><td>Direction / Type</td><td colspan="2">From the drop-down list, select the connection method for the VPN firewall:
• <b>Initiator</b>. The VPN firewall initiates the connection to the remote endpoint.
• <b>Responder</b>. The VPN firewall responds only to an IKE request from the remote endpoint.
• <b>Both</b>. The VPN firewall can both initiate a connection to the remote endpoint and respond to an IKE request from the remote endpoint.</td></tr>
<tr><td>Exchange Mode</td><td colspan="2">From the drop-down list, select the exchange mode between the VPN firewall and the remote VPN endpoint:
• <b>Main</b>. This mode is slower than the Aggressive mode but more secure.
• <b>Aggressive</b>. This mode is faster than the Main mode but less secure.
<b>Note:</b> If you specify either an FQDN or a User FQDN name as the local ID or remote ID (see the Local and Remote sections on the screen), the Aggressive mode is automatically selected.</td></tr>
</table>

Table 38. Add IKE Policy screen settings (continued)

<table>
<tr><th>Setting</th><th colspan="2">Description</th></tr>
<tr><td colspan="3"><b>Local</b></td></tr>
<tr><td>Select Local Gateway</td><td colspan="2">From the drop-down list, select one of the four WAN interfaces to function as the local gateway.</td></tr>
<tr><td rowspan="2">Identifier Type</td><td colspan="2">From the drop-down list, select one of the following ISAKMP identifiers to be used by the VPN firewall, and then specify the identifier in the field below:
• <b>Local WAN IP</b>. The WAN IP address of the VPN firewall. When you select this option, the Identifier field masks out.
• <b>FQDN</b>. The Internet address for the VPN firewall.
• <b>User FQDN</b>. The email address for a local VPN client or the VPN firewall.
• <b>DER ASN1 DN</b>. A distinguished name (DN) that identifies the VPN firewall in the DER encoding and ASN.1 format.</td></tr>
<tr><td>Identifier</td><td>Depending on the selection in the Identifier Type drop-down list, enter the IP address, email address, FQDN, or distinguished name.</td></tr>
<tr><td colspan="3"><b>Remote</b></td></tr>
<tr><td rowspan="2">Identifier Type</td><td colspan="2">From the drop-down list, select one of the following ISAKMP identifiers to be used by the remote endpoint, and then specify the identifier in the field below:
• <b>Remote WAN IP</b>. The WAN IP address of the remote endpoint. When you select this option, the Identifier field masks out.
• <b>FQDN</b>. The FQDN for a remote gateway.
• <b>User FQDN</b>. The email address for a remote VPN client or gateway.
• <b>DER ASN1 DN</b>. A distinguished name (DN) that identifies the remote endpoint in the DER encoding and ASN.1 format.</td></tr>
<tr><td>Identifier</td><td>Depending on the selection of the Identifier Type drop-down list, enter the IP address, email address, FQDN, or distinguished name.</td></tr>
<tr><td colspan="3"><b>IKE SA Parameters</b></td></tr>
<tr><td>Encryption Algorithm</td><td colspan="2">From the drop-down list, select one of the following five algorithms to negotiate the security association (SA):
• <b>DES</b>. Data Encryption Standard (DES).
• <b>3DES</b>. Triple DES. This is the default algorithm.
• <b>AES-128</b>. Advanced Encryption Standard (AES) with a 128-bits key size.
• <b>AES-192</b>. AES with a 192-bits key size.
• <b>AES-256</b>. AES with a 256-bits key size.</td></tr>
<tr><td>Authentication Algorithm</td><td colspan="2">From the drop-down list, select one of the following two algorithms to use in the VPN header for the authentication process:
• <b>SHA-1</b>. Hash algorithm that produces a 160-bit digest. This is the default setting.
• <b>MD5</b>. Hash algorithm that produces a 128-bit digest.</td></tr>
</table>

Table 38. Add IKE Policy screen settings (continued)

Setting	Description	
Authentication Method	Select one of the following radio buttons to specify the authentication method: • **Pre-shared key**. A secret that is shared between the VPN firewall and the remote endpoint. • **RSA-Signature**. Uses the active self certificate that you uploaded on the Certificates screen (see *Manage Self-Signed Certificates* on page 237). The pre-shared key is masked out when you select the RSA-Signature option.	
	Pre-shared key	A key with a minimum length of 8 characters no more than 49 characters. Do not use a double quote (“) in the key.
Diffie-Hellman (DH) Group	The DH Group sets the strength of the algorithm in bits. The higher the group, the more secure the exchange. From the drop-down list, select one of the following three strengths: • **Group 1 (768 bit)**. • **Group 2 (1024 bit)**. This is the default setting. • **Group 5 (1536 bit)**. **Note:** Ensure that the DH Group is configured identically on both sides.	
SA-Lifetime (sec)	The period in seconds for which the IKE SA is valid. When the period times out, rekeying occurs. The default is 28800 seconds (8 hours).	
Enable Dead Peer Detection **Note:** See also *Configure Keep-alives and Dead Peer Detection* on page 191.	Select a radio button to specify whether or not Dead Peer Detection (DPD) is enabled: • **Yes**. This feature is enabled. When the VPN firewall detects an IKE connection failure, it deletes the IPSec and IKE SA and forces a reestablishment of the connection. You need to specify the detection period in the Detection Period field and the maximum number of times that the VPN firewall attempts to reconnect in the Reconnect after failure count field. • **No**. This feature is disabled. This is the default setting.	
	Detection Period	The period in seconds between consecutive DPD R-U-THERE messages, which are sent only when the IPSec traffic is idle. The default is 10 seconds.
	Reconnect after failure count	The maximum number of DPD failures before the VPN firewall tears down the connection and then attempts to reconnect to the peer. The default is 3 failures.
Extended Authentication		
XAUTH Configuration **Note:** For more information about XAUTH and its authentication modes, see *Configure XAUTH for VPN Clients* on page 173.	Select one of the following radio buttons to specify whether or not Extended Authentication (XAUTH) is enabled, and, if enabled, which device is used to verify user account information: • **None**. XAUTH is disabled. This the default setting. • **Edge Device**. The VPN firewall functions as a VPN concentrator on which one or more gateway tunnels terminate. The authentication modes that are available for this configuration are User Database, RADIUS PAP, or RADIUS CHAP. • **IPSec Host**. The VPN firewall functions as a VPN client of the remote gateway. In this configuration the VPN firewall is authenticated by a remote gateway with a user name and password combination.	

Table 38. Add IKE Policy screen settings (continued)

Setting	Description	
XAUTH Configuration (continued)	Authentication Type	For an Edge Device configuration: from the drop-down list, select one of the following authentication types: • **User Database**. XAUTH occurs through the VPN firewall's user database. Users need to be added through the Add User screen (see *User Database Configuration* on page 174). • **Radius PAP**. XAUTH occurs through RADIUS Password Authentication Protocol (PAP). The local user database is first checked. If the user account is not present in the local user database, the VPN firewall connects to a RADIUS server. For more information, see *RADIUS Client Configuration* on page 174. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see *RADIUS Client Configuration* on page 174.
	Username	The user name for XAUTH.
	Password	The password for XAUTH.

4. Click **Apply** to save your settings. The IKE policy is added to the List of IKE Policies table.

➢ **To edit an IKE policy:**

1. Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display, with the IKE Policies screen in view (see *Figure 104* on page 160).
2. In the List of IKE Policies table, click the **Edit** table button to the right of the IKE policy that you want to edit. The Edit IKE Policy screen displays. This screen shows the same field as the Add IKE Policy screen (see *Figure 105* on page 161).
3. Modify the settings that you wish to change (see the previous table).
4. Click **Apply** to save your changes. The modified IKE policy is displayed in the List of IKE Policies table.

Configure VPN Policies

You can create two types of VPN policies. When you use the VPN Wizard to create a VPN policy, only the Auto method is available.

- **Manual**. You manually enter all settings (including the keys) for the VPN tunnel on the VPN firewall and on the remote VPN endpoint. No third-party server or organization is involved.
- **Auto**. Some settings for the VPN tunnel are generated automatically by using the IKE (Internet Key Exchange) Protocol to perform negotiations between the two VPN endpoints (the local ID endpoint and the remote ID endpoint). You still need to manually enter all settings on the remote VPN endpoint (unless the remote VPN endpoint also has a VPN Wizard).

In addition, a certification authority (CA) can also be used to perform authentication (see *Manage Digital Certificates* on page 234). To use a CA, each VPN gateway needs to have a certificate from the CA. For each certificate, there is both a public key and a private key. The public key is freely distributed, and is used by any sender to encrypt data intended for the receiver (the key owner). The receiver then uses its private key to decrypt the data (without the private key, decryption is impossible). The use of certificates for authentication reduces the amount of data entry that is required on each VPN endpoint.

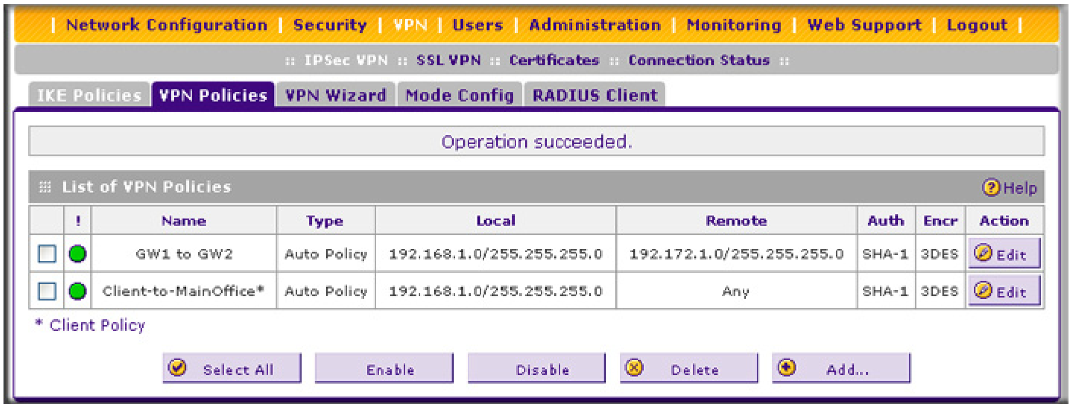
VPN Policies Screen

The VPN Policies screen allows you to add additional policies—either Auto or Manual—and to manage the VPN policies already created. You can edit policies, enable or disable policies, or delete them entirely. These are the rules for VPN policy use:

- Traffic covered by a policy is automatically sent via a VPN tunnel.
- When traffic is covered by two or more policies, the first matching policy is used. (In this situation, the order of the policies is important. However, if you have only one policy for each remote VPN endpoint, then the policy order is not important.)
- The VPN tunnel is created according to the settings in the security association (SA).
- The remote VPN endpoint needs to have a matching SA, otherwise it refuses the connection.

To access the VPN Policies screen:

Select **VPN > IPSec VPN > VPN Policies**. The VPN Policies screen displays. (The following figure shows some examples.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
?Help
Select All
Enable
Disable
Delete
Add...

Operation succeeded.

List of VPN Policies

	!	Name	Type	Local	Remote	Auth	Encr	Action
□	●	GW1 to GW2	Auto Policy	192.168.1.0/255.255.255.0	192.172.1.0/255.255.255.0	SHA-1	3DES	Edit
□	●	Client-to-MainOffice*	Auto Policy	192.168.1.0/255.255.255.0	Any	SHA-1	3DES	Edit

* Client Policy

Figure 106.

Each policy contains the data that are explained in the following table. These fields are explained in more detail in *Table 40* on page 169.

Table 39. VPN Policies screen information

Item	Description
! (Status)	Indicates whether the policy is enabled (green circle) or disabled (gray circle). To enable or disable a policy, select the check box adjacent to the circle and click the **Enable** or **Disable** table button, as appropriate.
Name	The name that identifies the VPN policy. When you use the VPN Wizard to create a VPN policy, the name of the VPN policy (and of the automatically created accompanying IKE policy) is the connection name.
Type	Auto or Manual as described previously (Auto is used during VPN Wizard configuration).
Local	IP address (either a single address, range of addresses, or subnet address) on your LAN. Traffic needs to be from (or to) these addresses to be covered by this policy. (The subnet address is supplied as the default IP address when you are using the VPN Wizard).
Remote	IP address or address range of the remote network. Traffic needs to be to (or from) these addresses to be covered by this policy. (The VPN Wizard default requires the remote LAN IP address and subnet mask.)
Auth	The authentication algorithm that is used for the VPN tunnel. This setting needs to match the setting on the remote endpoint.
Encr	The encryption algorithm that is used for the VPN tunnel. This setting needs to match the setting on the remote endpoint.

➢ To delete one or more VPN polices:

1. Select the check box to the left of the policy that you want to delete, or click the **Select All** table button to select all VPN policies.
2. Click the **Delete** table button.

➢ To enable or disable one ore more VPN policies:

1. Select the check box to the left of the policy that you want to delete, or click the **Select All** table button to select all IKE Policies.
2. Click the **Enable** or **Disable** table button.

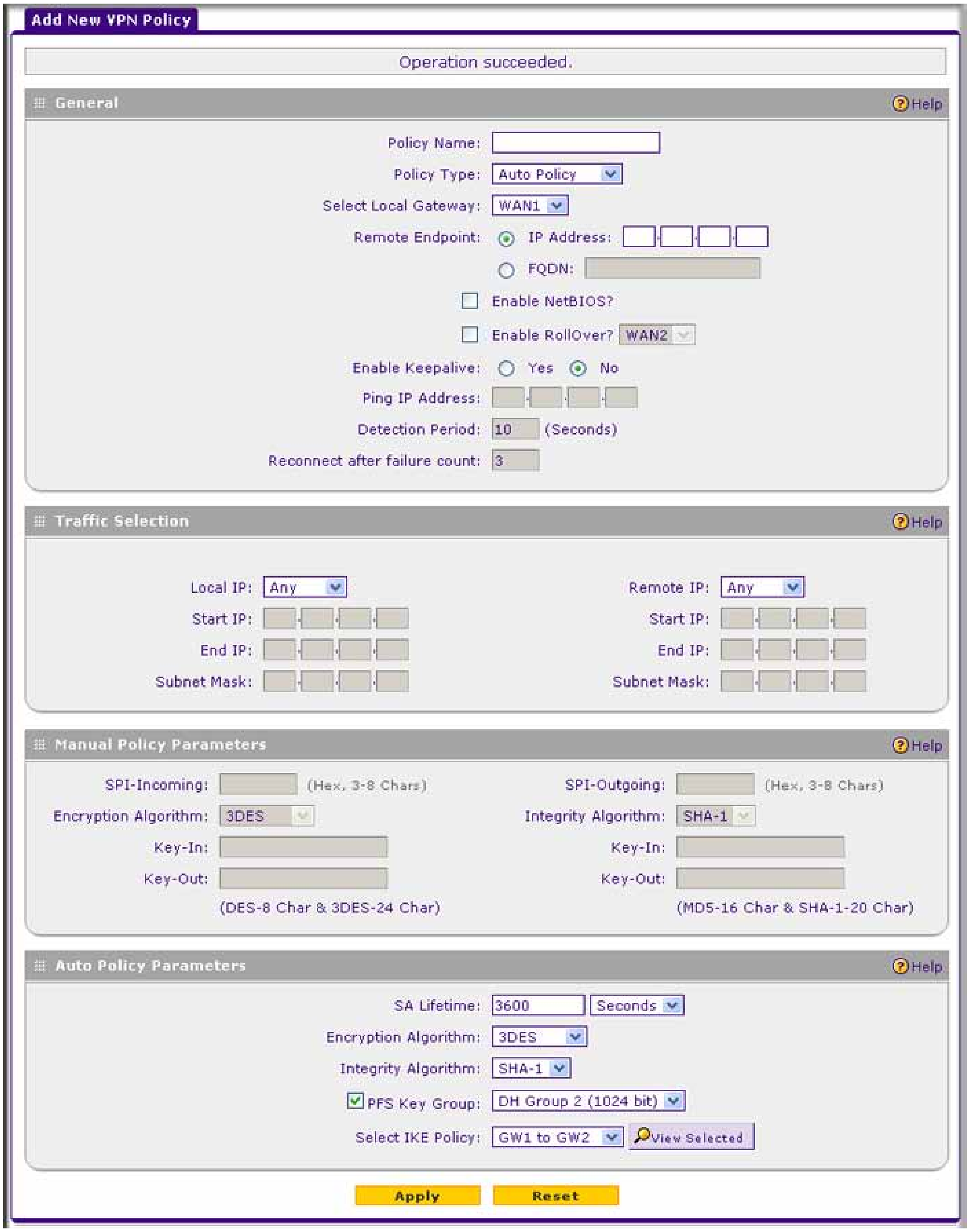
For information about how to add or edit a VPN policy, see the next section, *Manually Add or Edit a VPN Policy*.

Note: You cannot delete or edit an IKE policy for which the VPN policy is active. You first need to disable or delete the VPN policy before you can delete or edit the IKE policy.

Manually Add or Edit a VPN Policy

➢ **To manually add a VPN policy:**

1. Select **VPN > IPSec VPN > VPN Policies**. The VPN Policies screen displays (see *Figure 106* on page 166).
2. Under the List of VPN Policies table, click the **Add** table button. The Add New VPN Policy screen displays:



Add New VPN Policy

Operation succeeded.

General

Policy Name:
Policy Type: Auto Policy
Select Local Gateway: WAN1
Remote Endpoint: ● IP Address: ○ FQDN:
□ Enable NetBIOS?
□ Enable RollOver? WAN2
Enable Keepalive: ○ Yes ● No
Ping IP Address:
Detection Period: 10 (Seconds)
Reconnect after failure count: 3

Traffic Selection

Local IP: Any
Start IP:
End IP:
Subnet Mask:

Remote IP: Any
Start IP:
End IP:
Subnet Mask:

Manual Policy Parameters

SPI-Incoming: (Hex, 3-8 Chars)
Encryption Algorithm: 3DES
Key-In:
Key-Out:
(DES-8 Char & 3DES-24 Char)

SPI-Outgoing: (Hex, 3-8 Chars)
Integrity Algorithm: SHA-1
Key-In:
Key-Out:
(MD5-16 Char & SHA-1-20 Char)

Auto Policy Parameters

SA Lifetime: 3600 Seconds
Encryption Algorithm: 3DES
Integrity Algorithm: SHA-1
☑ PFS Key Group: DH Group 2 (1024 bit)
Select IKE Policy: GW1 to GW2

Figure 107.

3. Complete the settings as explained the following table:

Table 40. Add New VPN Policy screen settings

<table>
<tr><th>Setting</th><th colspan="2">Description</th></tr>
<tr><td colspan="3"><b>General</b></td></tr>
<tr><td>Policy Name</td><td colspan="2">A descriptive name of the VPN policy for identification and management purposes.
<b>Note:</b> The name is not supplied to the remote VPN endpoint.</td></tr>
<tr><td>Policy Type</td><td colspan="2">From the drop-down list, select one of the following policy types:
• <b>Auto Policy</b>. Some settings (the ones in the Manual Policy Parameters section of the screen) for the VPN tunnel are generated automatically.
• <b>Manual Policy</b>. All settings need to be specified, including the ones in the Manual Policy Parameters section of the screen.</td></tr>
<tr><td>Select Local Gateway</td><td colspan="2">From the drop-down list, select one of the four WAN interfaces to function as the local gateway.</td></tr>
<tr><td>Remote Endpoint</td><td colspan="2">Select a radio button to specify how the remote endpoint is defined:
• <b>IP Address</b>. Enter the IP address of the remote endpoint in the fields to the right of the radio button.
• <b>FQDN</b>. Enter the FQDN of the remote endpoint in the field to the right of the radio button.</td></tr>
<tr><td>Enable NetBIOS?</td><td colspan="2">Select this check box to allow NetBIOS broadcasts to travel over the VPN tunnel. For more information about NetBIOS, see <i>Configure NetBIOS Bridging with IPSec VPN</i> on page 194. This feature is disabled by default.</td></tr>
<tr><td>Enable RollOver?</td><td colspan="2">If you have configured the VPN firewall to function in WAN auto-rollover mode (see <i>Configure the Auto-Rollover Mode and Failure Detection Method</i> on page 34), select the <b>Enable RollOver?</b> check box. Then, from the corresponding drop-down list, select the backup WAN interface. After an auto-rollover has occurred, the VPN tunnel will be reestablished using the backup WAN interface. This feature is disabled by default.</td></tr>
<tr><td rowspan="4">Enable Keepalive
<b>Note:</b> See also <i>Configure Keep-alives and Dead Peer Detection</i> on page 191.</td><td colspan="2">Select a radio button to specify if keep-alive is enabled:
• <b>Yes</b>. This feature is enabled. Periodically, the VPN firewall sends keep-alive requests (ping packets) to the remote endpoint to keep the tunnel alive. You need to specify the ping IP address in the Ping IP Address field, detection period in the Detection Period field, and the maximum number of keep-alive requests that the VPN firewall sends in the Reconnect after failure count field.
• <b>No</b>. This feature is disabled. This is the default setting.</td></tr>
<tr><td>Ping IP Address</td><td>The IP address that the VPN firewall pings. The address needs to be of a host that can respond to ICMP ping requests.</td></tr>
<tr><td>Detection Period</td><td>The period in seconds between the keep-alive requests. The default setting is 10 seconds.</td></tr>
<tr><td>Reconnect after failure count</td><td>The maximum number of keep-alive requests before the VPN firewall tears down the connection and then attempts to reconnect to the remote endpoint. The default is 3 keep-alive requests.</td></tr>
</table>

Table 40. Add New VPN Policy screen settings (continued)

Setting	Description
Traffic Selection	
Local IP	From the drop-down list, select the address or addresses that are part of the VPN tunnel on the VPN firewall: • **Any**. All PCs and devices on the network. • **Single**. A single IP address on the network. Enter the IP address in the Start IP Address field. • **Range**. A range of IP addresses on the network. Enter the starting IP address in the Start IP Address field and the ending IP address in the End IP Address field. • **Subnet**. A subnet on the network. Enter the starting IP address in the Start IP Address field and the subnet mask in the Subnet Mask field. **Note:** You cannot select Any for both the VPN firewall and the remote endpoint.
Remote IP	From the drop-down list, select the address or addresses that are part of the VPN tunnel on the remote endpoint. The menu choices are the same as for the Local IP drop-down list.
Manual Policy Parameters **Note:** These fields apply only when you select Manual Policy as the policy type. When you specify the settings for the fields in this section, a security association (SA) is created.	
SPI-Incoming	The Security Parameters Index (SPI) for the inbound policy. Enter a hexadecimal value between 3 and 8 characters (for example: 0x1234).
Encryption Algorithm	From the drop-down list, select one of the following five algorithms to negotiate the security association (SA): • **DES**. Data Encryption Standard (DES). • **3DES**. Triple DES. This is the default algorithm. • **AES-128**. Advanced Encryption Standard (AES) with a 128-bits key size. • **AES-192**. AES with a 192-bits key size. • **AES-256**. AES with a 256-bits key size.
Key-In	The encryption key for the inbound policy. The length of the key depends on the selected encryption algorithm: • **DES**. Enter 8 characters. • **3DES**. Enter 24 characters. • **AES-128**. Enter 16 characters. • **AES-192**. Enter 24 characters. • **AES-256**. Enter 32 characters.
Key-Out	The encryption key for the outbound policy. The length of the key depends on the selected encryption algorithm: • **DES**. Enter 8 characters. • **3DES**. Enter 24 characters. • **AES-128**. Enter 16 characters. • **AES-192**. Enter 24 characters. • **AES-256**. Enter 32 characters.

Table 40. Add New VPN Policy screen settings (continued)

Setting	Description
SPI-Outgoing	The Security Parameters Index (SPI) for the outbound policy. Enter a hexadecimal value between 3 and 8 characters (for example: 0x1234).
Integrity Algorithm	From the drop-down list, select one of the following two algorithms to be used in the VPN header for the authentication process: • **SHA-1**. Hash algorithm that produces a 160-bit digest. This is the default setting. • **MD5**. Hash algorithm that produces a 128-bit digest.
Key-In	The integrity key for the inbound policy. The length of the key depends on the selected integrity algorithm: • **MD5**. Enter 16 characters. • **SHA-1**. Enter 20 characters.
Key-Out	The integrity key for he outbound policy. The length of the key depends on the selected integrity algorithm: • **MD5**. Enter 16 characters. • **SHA-1**. Enter 20 characters.
Auto Policy Parameters **Note:** These fields apply only when you select Auto Policy as the policy type.	
SA Lifetime	The lifetime of the security association (SA) is the period or the amount of transmitted data after which the SA becomes invalid and needs to be renegotiated. From the drop-down list, select how the SA lifetime is specified: • **Seconds**. In the SA Lifetime field, enter a period in seconds. The minimum value is 300 seconds. The default value is 3600 seconds. • **KBytes**. In the SA Lifetime field, enter a number of kilobytes. The minimum value is 1920000 KB.
Encryption Algorithm	From the drop-down list, select one of the following five algorithms to negotiate the security association (SA): • **DES**. Data Encryption Standard (DES). • **3DES**. Triple DES. This is the default algorithm. • **AES-128**. Advanced Encryption Standard (AES) with a 128-bits key size. • **AES-192**. AES with a 192-bits key size. • **AES-256**. AES with a 256-bits key size.
Integrity Algorithm	From the drop-down list, select one of the following two algorithms to be used in the VPN header for the authentication process: • **SHA-1**. Hash algorithm that produces a 160-bit digest. This is the default setting. • **MD5**. Hash algorithm that produces a 128-bit digest.

Table 40. Add New VPN Policy screen settings (continued)

Setting	Description
PFS Key Group	Select this check box to enable Perfect Forward Secrecy (PFS), and then select a Diffie-Hellman (DH) group from the drop-down list. The DH Group sets the strength of the algorithm in bits. The higher the group, the more secure the exchange. From the drop-down list, select one of the following three strengths: • **Group 1 (768 bit)**. • **Group 2 (1024 bit)**. This is the default setting. • **Group 5 (1536 bit)**.
Select IKE Policy	Select an existing IKE policy that defines the characteristics of the Phase-1 negotiation. Click the **View Selected** button to display the selected IKE policy.

4. Click **Apply** to save your settings. The VPN policy is added to the List of VPN Policies table.

➤ **To edit a VPN policy:**

1. Select **VPN > IPSec VPN > VPN Policies**. The VPN Policies screen displays (see *Figure 106* on page 166).
2. In the List of VPN Policies table, click the **Edit** table button to the right of the VPN policy that you want to edit. The Edit VPN Policy screen displays. This screen shows the same fields as the Add New VPN Policy screen (see *Figure 107* on page 168).
3. Modify the settings that you wish to change (see the previous table).
4. Click **Apply** to save your changes. The modified VPN policy is displayed in the List of VPN Policies table.

Configure Extended Authentication (XAUTH)

When many VPN clients connect to a VPN firewall, you might want to use a unique user authentication method beyond relying on a single common pre-shared key for all clients. Although you could configure a unique VPN policy for each user, it is more efficient to authenticate users from a stored list of user accounts. XAUTH provides the mechanism for requesting individual authentication information from the user, and a local user database or an external authentication server, such as a RADIUS server, provides a method for storing the authentication information centrally in the local network.

You can enable XAUTH when you manually add or edit an IKE policy. Two types of XAUTH are available:

- **Edge Device**. The VPN firewall is used as a VPN concentrator on which one or more gateway tunnels terminate. You need to specify the authentication type that should be used during verification of the credentials of the remote VPN gateways: User Database, RADIUS-PAP, or RADIUS-CHAP.
- **IPSec Host**. Authentication by the remote gateway through a user name and password that are associated with the IKE policy. The user name and password that are used to authenticate the VPN firewall need to be specified on the remote gateway.

Note: If a RADIUS-PAP server is enabled for authentication, XAUTH first checks the local user database for the user credentials. If the user account is not present, the VPN firewall then connects to a RADIUS server.

Configure XAUTH for VPN Clients

Once the XAUTH has been enabled, you need to establish user accounts in the user database to be authenticated against XAUTH, or you need to enable a RADIUS-CHAP or RADIUS-PAP server.

Note: You cannot modify an existing IKE policy to add XAUTH while the IKE policy is in use by a VPN policy. The VPN policy needs to be disabled before you can modify the IKE policy.

➢ **To enable and configure XAUTH:**

1. Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display, with the IKE Policies screen in view (see *Figure 104* on page 160).
2. In the List of IKE Policies table, click the **Edit** table button to the right of the IKE policy for which you want to enable and configure XAUTH. The Edit IKE Policy screen displays. This screen shows the same fields as the Add IKE Policy screen (see *Figure 105* on page 161).
3. In the Extended Authentication section of the screen, complete the settings as explained the following table:

Table 41. Extended authentication settings

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td colspan="2">Select one of the following radio buttons to specify whether or not Extended Authentication (XAUTH) is enabled, and, if enabled, which device is used to verify user account information:
• <b>None</b>. XAUTH is disabled. This the default setting.
• <b>Edge Device</b>. The VPN firewall functions as a VPN concentrator on which one or more gateway tunnels terminate. The authentication modes that are available for this configuration are User Database, RADIUS PAP, or RADIUS CHAP.
• <b>IPSec Host</b>. The VPN firewall functions as a VPN client of the remote gateway. In this configuration the VPN firewall is authenticated by a remote gateway with a user name and password combination.</td></tr>
</table>

Table 41. Extended authentication settings (continued)

Setting	Description
Authentication Type	For an Edge Device configuration: from the drop-down list, select one of the following authentication types: • **User Database**. XAUTH occurs through the VPN firewall's user database. You can add users on the Add User screen (see *User Database Configuration* on page 174). • **Radius PAP**. XAUTH occurs through RADIUS Password Authentication Protocol (PAP). The local user database is first checked. If the user account is not present in the local user database, the VPN firewall connects to a RADIUS server. For more information, see *RADIUS Client Configuration* on page 174. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see *RADIUS Client Configuration* on page 174.
Username	The user name for XAUTH.
Password	The password for XAUTH.

4. Click **Apply** to save your settings.

User Database Configuration

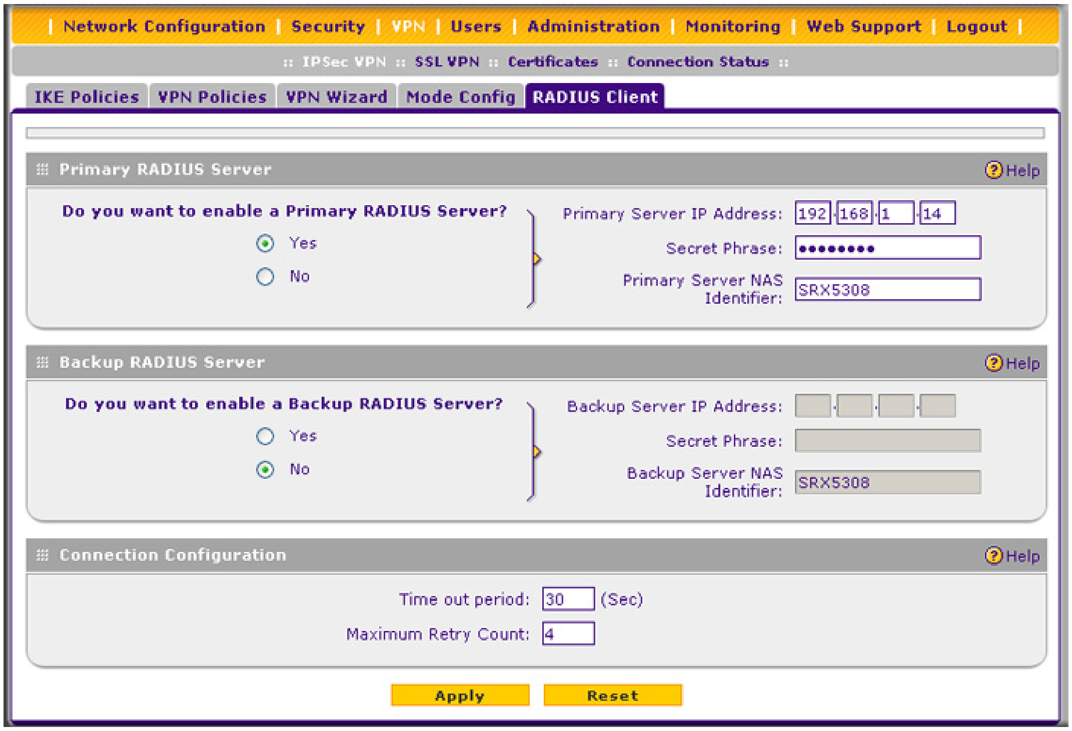
When XAUTH is enabled in an Edge Device configuration, users are authenticated either through a local user database account or by an external RADIUS server. Whether or not you use a RADIUS server, you might want some users to be authenticated locally. These users need to be added to the List of Users table on the Users screen, as described in *Configure User Accounts* on page 227.

RADIUS Client Configuration

Remote Authentication Dial In User Service (RADIUS, RFC 2865) is a protocol for managing authentication, authorization, and accounting (AAA) of multiple users in a network. A RADIUS server stores a database of user information, and can validate a user at the request of a gateway or server in the network when a user requests access to network resources. During the establishment of a VPN connection, the VPN gateway can interrupt the process with an XAUTH request. At that point, the remote user needs to provide authentication information such as a user name and password or some encrypted response using his or her user name and password information. The gateway then attempts to verify this information first against a local user database (if RADIUS-PAP is enabled) and then by relaying the information to a central authentication server such as a RADIUS server.

➢ **To configure primary and backup RADIUS servers:**

1. Select **VPN > IPSec VPN > RADIUS Client**. The RADIUS Client screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
Help
Help
Help
Apply
Reset

Primary RADIUS Server

Do you want to enable a Primary RADIUS Server?

● Yes

○ No

Primary Server IP Address: 192 . 168 . 1 . 14

Secret Phrase: ••••••••

Primary Server NAS Identifier: SRX5308

Backup RADIUS Server

Do you want to enable a Backup RADIUS Server?

○ Yes

● No

Backup Server IP Address: . . .

Secret Phrase:

Backup Server NAS Identifier: SRX5308

Connection Configuration

Time out period: 30 (Sec)

Maximum Retry Count: 4

Figure 108.

2. Complete the settings as explained the following table:

Table 42. RADIUS Client screen settings

Settings	Description
Primary RADIUS Server	
Select the **Yes** radio button to enable and configure the primary RADIUS server, and then enter the settings for the three fields to the right. The default setting is that the **No** radio button is selected.	
Primary Server IP Address	The IP address of the primary RADIUS server.
Secret Phrase	A shared secret phrase to authenticate the transactions between the client and the primary RADIUS server. The same secret phrase needs to be configured on both the client and the server.
Primary Server NAS Identifier	The primary Network Access Server (NAS) identifier that needs to be present in a RADIUS request. **Note:** The VPN firewall functions as a NAS, allowing network access to external users after verification of their authentication information. In a RADIUS transaction, the NAS needs to provide a NAS identifier information to the RADIUS server. Depending on the configuration of the RADIUS server, the VPN firewall's IP address might be sufficient as an identifier, or the server might require a name, which you need to enter in this field.
Backup RADIUS Server	
Select the **Yes** radio button to enable and configure the backup RADIUS server, and then enter the settings for the three fields to the right. The default setting is that the **No** radio button is selected.	

Table 42. RADIUS Client screen settings (continued)

Settings	Description
Backup Server IP Address	The IP address of the backup RADIUS server.
Secret Phrase	A shared secret phrase to authenticate the transactions between the client and the backup RADIUS server. The same secret phrase needs to be configured on both the client and the server.
Backup Server NAS Identifier	The backup NAS identifier that needs to be present in a RADIUS request. **Note:** See the note earlier in this table for the Primary Server NAS Identifier.
Connection Configuration	
Time out period	The period in seconds that the VPN firewall waits for a response from a RADIUS server.
Maximum Retry Counts	The maximum number of times that the VPN firewall attempts to connect to a RADIUS server.

3. Click **Apply** to save your settings.

Note: You select the RADIUS authentication protocol (PAP or CHAP) on the Edit IKE Policy screen or Add IKE Policy screen (see *Configure XAUTH for VPN Clients* on page 173).

Assign IP Addresses to Remote Users (Mode Config)

To simplify the process of connecting remote VPN clients to the VPN firewall, use the Mode Config feature to assign IP addresses to remote users, including a network access IP address, subnet mask, WINS server, and DNS address from the VPN firewall. Remote users are given IP addresses available in a secured network space so that remote users appear as seamless extensions of the network.

Mode Config Operation

After the IKE Phase 1 negotiation is complete, the VPN connection initiator (which is the remote user with a VPN client) requests the IP configuration settings such as the IP address, subnet mask, WINS server, and DNS address from the VPN firewall. The Mode Config feature allocates an IP address from the configured IP address pool and activates a temporary IPSec policy, using the information that is specified in the Traffic Tunnel Security Level section of the Mode Config record (on the Add Mode Config Record screen that is shown in *Figure 110* on page 178).

Note: After configuring a Mode Config record, you need to manually configure an IKE policy and select the newly created Mode Config record from the Select Mode Config Record drop-down list (see *Configure Mode Config Operation on the VPN Firewall* on page 177). You do not need to make changes to any VPN policy.

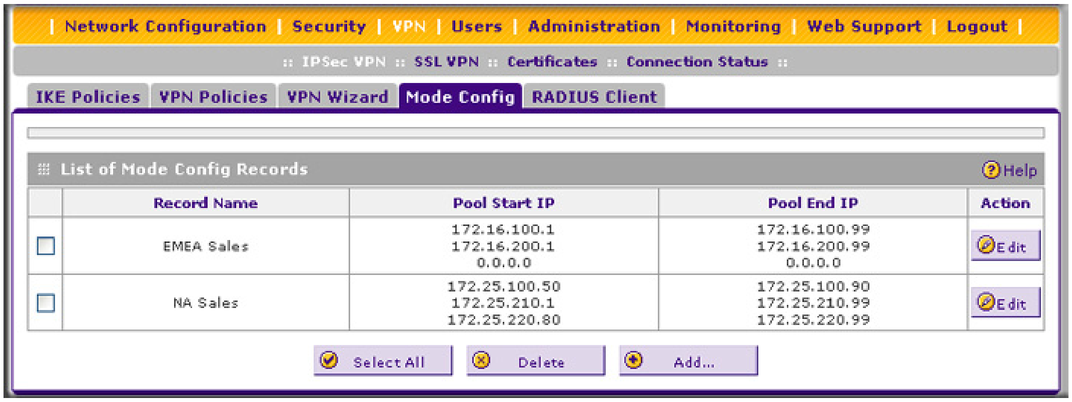
Note: An IP address that is allocated to a VPN client is released only after the VPN client has gracefully disconnected or after the SA liftetime for the connection has timed out.

Configure Mode Config Operation on the VPN Firewall

To configure Mode Config on the VPN firewall, first create a Mode Config record, and then select the Mode Config record for an IKE policy.

➢ **To configure Mode Config on the VPN firewall:**

1. Select **VPN > IPSec VPN > Mode Config**. The Mode Config screen displays:



| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
Help
Select All
Delete
Add...

List of Mode Config Records

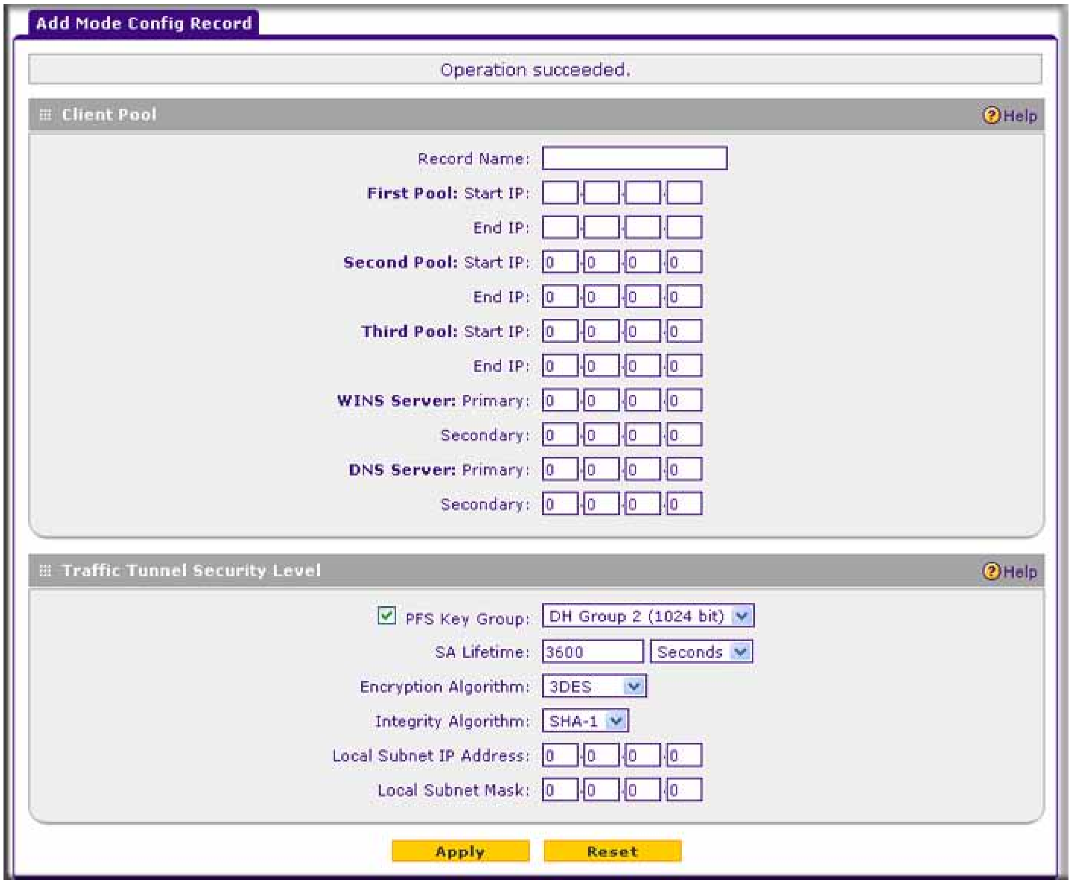
	Record Name	Pool Start IP	Pool End IP	Action
□	EMEA Sales	172.16.100.1 172.16.200.1 0.0.0.0	172.16.100.99 172.16.200.99 0.0.0.0	Edit
□	NA Sales	172.25.100.50 172.25.210.1 172.25.220.80	172.25.100.90 172.25.210.99 172.25.220.99	Edit

Figure 109.

As an example, the screen shows two Mode Config records with the names EMEA Sales and NA Sales:

- For EMEA Sales, a first pool (172.16.100.1 through 172.16.100.99) and second pool (172.16.200.1 through 172.16.200.99) are shown.
- For NA Sales, a first pool (172.25.100.50 through 172.25.100.90), a second pool (172.25.210.1 through 172.25.210.99), and a third pool (172.25.220.80 through 172.25.220.99) are shown.

2. Under the List of Mode Config Records table, click the **Add** table button. The Add Mode Config Record screen displays:



Add Mode Config Record

Operation succeeded.

Client Pool

Record Name:

First Pool: Start IP:

End IP:

Second Pool: Start IP: 0 . 0 . 0 . 0

End IP: 0 . 0 . 0 . 0

Third Pool: Start IP: 0 . 0 . 0 . 0

End IP: 0 . 0 . 0 . 0

WINS Server: Primary: 0 . 0 . 0 . 0

Secondary: 0 . 0 . 0 . 0

DNS Server: Primary: 0 . 0 . 0 . 0

Secondary: 0 . 0 . 0 . 0

Traffic Tunnel Security Level

☑ PFS Key Group: DH Group 2 (1024 bit)

SA Lifetime: 3600 Seconds

Encryption Algorithm: 3DES

Integrity Algorithm: SHA-1

Local Subnet IP Address: 0 . 0 . 0 . 0

Local Subnet Mask: 0 . 0 . 0 . 0

Figure 110.

3. Complete the settings as explained the following table:

Table 43. Add Mode Config Record screen settings

Settings	Description
Client Pool	
Record Name	A descriptive name of the Mode Config record for identification and management purposes.
First Pool	Assign at least one range of IP pool addresses in the First Pool fields to enable the VPN firewall to allocate these to remote VPN clients. The Second Pool and Third Pool fields are optional To specify any client pool, enter the starting IP address for the pool in the Start IP field and enter the ending IP address for the pool in the End IP field. **Note:** No IP pool should be within the local network IP addresses. Use a different range of private IP addresses such as 172.173.xxx.xx.
Second Pool	
Third Pool	
WINS Server	If there is a WINS server on the local network, enter its IP address in the Primary field. You can enter the IP address of a second WINS server in the Secondary field.

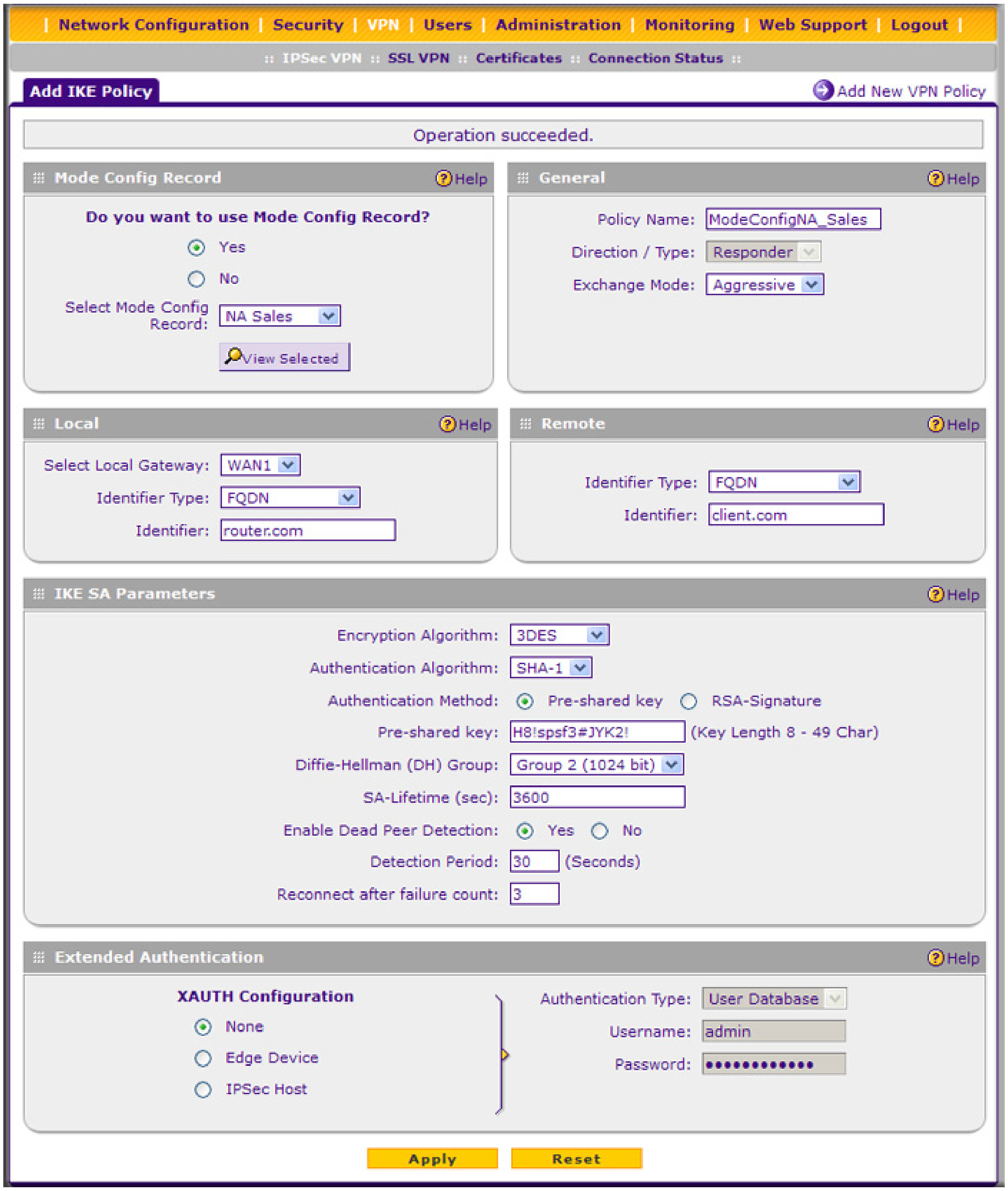
Table 43. Add Mode Config Record screen settings (continued)

Settings	Description
DNS Server	Enter the IP address of the DNS server that is used by remote VPN clients in the Primary field. You can enter the IP address of a second DNS server in the Secondary field.
Traffic Tunnel Security Level **Note:** Generally, the default settings work well for a Mode Config configuration.	
PFS Key Group	Select this check box to enable Perfect Forward Secrecy (PFS), and then select a Diffie-Hellman (DH) group from the drop-down list. The DH Group sets the strength of the algorithm in bits. The higher the group, the more secure the exchange. From the drop-down list, select one of the following three strengths: • **Group 1 (768 bit)** • **Group 2 (1024 bit)**. This is the default setting. • **Group 5 (1536 bit)**
SA Lifetime	The lifetime of the security association (SA) is the period or the amount of transmitted data after which the SA becomes invalid and needs to be renegotiated. From the drop-down list, select how the SA lifetime is specified: • **Seconds**. In the SA Lifetime field, enter a period in seconds. The minimum value is 300 seconds. The default value is 3600 seconds. • **KBytes**. In the SA Lifetime field, enter a number of kilobytes. The minimum value is 1920000 KB.
Encryption Algorithm	From the drop-down list, select one of the following five algorithms to negotiate the security association (SA): • **DES**. Data Encryption Standard (DES). • **3DES**. Triple DES. This is the default algorithm. • **AES-128**. Advanced Encryption Standard (AES) with a 128-bits key size. • **AES-192**. AES with a 192-bits key size. • **AES-256**. AES with a 256-bits key size.
Integrity Algorithm	From the drop-down list, select one of the following two algorithms to be used in the VPN header for the authentication process: • **SHA-1**. Hash algorithm that produces a 160-bit digest. This is the default setting. • **MD5**. Hash algorithm that produces a 128-bit digest.
Local IP Address	The local IP address to which remote VPN clients have access. If you do not specify a local IP address, the VPN firewall’s default LAN IP address is used (by default, 192.168.1.1).
Local Subnet Mask	The local subnet mask. Typically, this is 255.255.255.0.

4. Click **Apply** to save your settings. The new Mode Config record is added to the List of Mode Config Records table.

   Continue the Mode Config configuration procedure by configuring an IKE policy.

5. Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display, with the IKE Policies screen in view (see *Figure 104* on page 160).
6. Under the List of IKE Policies table, click the **Add** table button. The Add IKE Policy screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: Certificates :: Connection Status ::
Add IKE Policy
Add New VPN Policy
Help
View Selected
Apply
Reset

Operation succeeded.

Mode Config Record

Do you want to use Mode Config Record?

● Yes ○ No

Select Mode Config Record: NA Sales

General

Policy Name: ModeConfigNA_Sales

Direction / Type: Responder

Exchange Mode: Aggressive

Local

Select Local Gateway: WAN1

Identifier Type: FQDN

Identifier: router.com

Remote

Identifier Type: FQDN

Identifier: client.com

IKE SA Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

Authentication Method: ● Pre-shared key ○ RSA-Signature

Pre-shared key: H8!spsf3#JYK2! (Key Length 8 - 49 Char)

Diffie-Hellman (DH) Group: Group 2 (1024 bit)

SA-Lifetime (sec): 3600

Enable Dead Peer Detection: ● Yes ○ No

Detection Period: 30 (Seconds)

Reconnect after failure count: 3

Extended Authentication

XAUTH Configuration

● None

○ Edge Device

○ IPSec Host

Authentication Type: User Database

Username: admin

Password: ••••••••••••

Figure 111.

7. On the Add IKE Policy screen, complete the settings as explained the following table.

Note: The settings that are explained in the following table are specifically for a Mode Config configuration. *Table 38* on page 162 explains the general IKE policy settings.

Table 44. Add IKE Policy screen settings for a Mode Config configuration

Settings	Description	
Mode Config Record		
Do you want to use Mode Config Record?	Select the **Yes** radio button. **Note:** Because Mode Config functions only in Aggressive mode, selecting the **Yes** radio button sets the tunnel exchange mode to Aggressive mode and disables the Main mode. Mode Config also requires that both the local and remote ends are defined by their FQDNs.	
	Select Mode Config Record	From the drop-down list, select the Mode Config record that you created in *step 4* on 179. In this example, we are using NA Sales.
General		
Policy Name	A descriptive name of the IKE policy for identification and management purposes. In this example, we are using ModeConfigNA_Sales. **Note:** The name is not supplied to the remote VPN endpoint.	
Direction / Type	Responder is automatically selected when you select the **Yes** radio button in the Mode Config Record section of the screen. This ensures that the VPN firewall responds to an IKE request from the remote endpoint but does not initiate one.	
Exchange Mode	Aggressive mode is automatically selected you select the **Yes** radio button in the Mode Config Record section of the screen.	
Local		
Select Local Gateway	From the drop-down list, select one of the four WAN interfaces to function as the local gateway.	
Identifier Type	From the drop-down list, select **FQDN**. **Note:** Mode Config requires that the VPN firewall (that is, the local end) is defined by an FQDN.	
	Identifier	Enter an FQDN for the VPN firewall. In this example, we are using router.com.

Table 44. Add IKE Policy screen settings for a Mode Config configuration (continued)

Settings	Description	
Remote		
Identifier Type	From the drop-down list, select **FQDN**. **Note:** Mode Config requires that the remote end is defined by an FQDN.	
	Identifier	Enter the FQDN for the remote end. This needs to be an FQDN that is not used in any other IKE policy. In this example, we are using client.com.
IKE SA Parameters **Note:** Generally, the default settings work well for a Mode Config configuration.		
Encryption Algorithm	From the drop-down list, select the **3DES** algorithm to negotiate the security association (SA).	
Authentication Algorithm	From the drop-down list, select the **SHA-1** algorithm to be used in the VPN header for the authentication process.	
Authentication Method	Select **Pre-shared key** as the authentication method, and enter a key in the Pre-shared key field.	
	Pre-shared key	A key with a minimum length of 8 characters and no more than 49 characters. Do not use a double quote (“) in the key. In this example, we are using H8!spsf3#JYK2!.
Diffie-Hellman (DH) Group	The DH Group sets the strength of the algorithm in bits. From the drop-down list, select **Group 2 (1024 bit)**.	
SA-Lifetime (sec)	The period in seconds for which the IKE SA is valid. When the period times out, the next rekeying needs to occur. The default is 28800 seconds (8 hours). However, for a Mode Config configuration, NETGEAR recommends 3600 seconds (1 hour).	
Enable Dead Peer Detection **Note:** See also *Configure Keep-alives and Dead Peer Detection* on page 191.	Select a radio button to specify whether or not Dead Peer Detection (DPD) is enabled: • **Yes**. This feature is enabled. When the VPN firewall detects an IKE connection failure, it deletes the IPSec and IKE SA and forces a reestablishment of the connection. You need to specify the detection period in the Detection Period field and the maximum number of times that the VPN firewall attempts to reconnect in the Reconnect after failure count field. • **No**. This feature is disabled. This is the default setting.	
	Detection Period	The period in seconds between consecutive DPD R-U-THERE messages, which are sent only when the IPSec traffic is idle. The default setting is 10 seconds. In this example, we are using 30 seconds.
	Reconnect after failure count	The maximum number of DPD failures before the VPN firewall tears down the connection and then attempts to reconnect to the peer. The default is 3 failures.

Table 44. Add IKE Policy screen settings for a Mode Config configuration (continued)

Settings	Description	
Extended Authentication		
XAUTH Configuration **Note:** For more information about XAUTH and its authentication modes, see *Configure XAUTH for VPN Clients* on page 173.	Select one of the following radio buttons to specify whether or not Extended Authentication (XAUTH) is enabled, and, if enabled, which device is used to verify user account information: • **None**. XAUTH is disabled. This the default setting. • **Edge Device**. The VPN firewall functions as a VPN concentrator on which one or more gateway tunnels terminate. The authentication modes that are available for this configuration are User Database, RADIUS PAP, or RADIUS CHAP. • **IPSec Host**. The VPN firewall functions as a VPN client of the remote gateway. In this configuration the VPN firewall is authenticated by a remote gateway with a user name and password combination.	
	Authentication Type	For an Edge Device configuration: From the drop-down list, select one of the following authentication types: • **User Database**. XAUTH occurs through the VPN firewall's user database. You can add users on the Add User screen (see *User Database Configuration* on page 174). • **Radius PAP**. XAUTH occurs through RADIUS Password Authentication Protocol (PAP). The local user database is first checked. If the user account is not present in the local user database, the VPN firewall connects to a RADIUS server. For more information, see *RADIUS Client Configuration* on page 174. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see *RADIUS Client Configuration* on page 174.
	Username	The user name for XAUTH.
	Password	The password for XAUTH.

8. Click **Apply** to save your settings. The IKE policy is added to the List of IKE Policies table.

Configure the NETGEAR VPN Client for Mode Config Operation

When the Mode Config feature is enabled, the following information is negotiated between the VPN client and the VPN firewall during the authentication phase:

- Virtual IP address of the VPN client
- DNS server address (optional)
- WINS server address (optional)

The virtual IP address that is issued by the VPN firewall is displayed in the VPN Client Address field on the VPN client's IPSec pane.

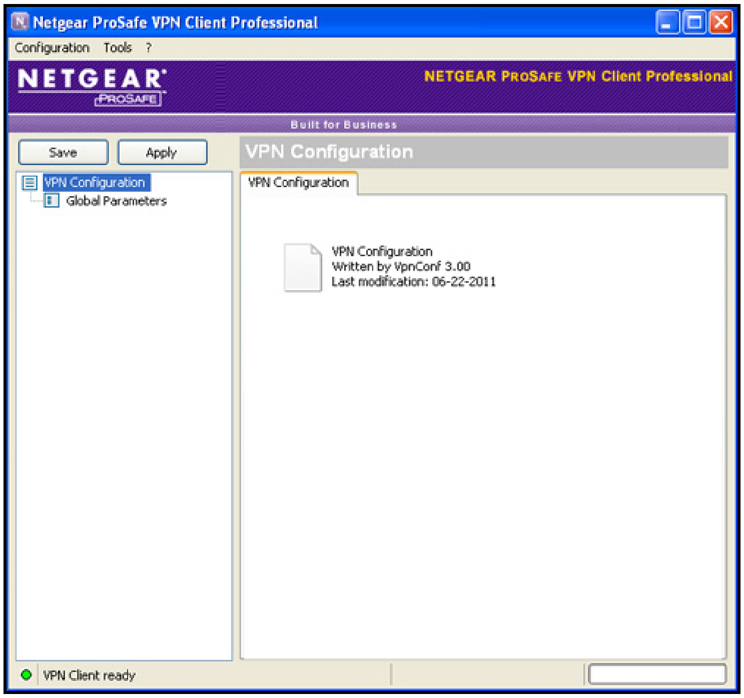
Note: Perform these tasks from a PC that has the NETGEAR ProSafe VPN Client installed.

To configure the VPN client for Mode Config operation, create authentication settings (phase 1 settings), create an associated IPSec configuration (phase 2 settings), and then specify the global parameters.

Configure the Mode Config Authentication Settings (Phase 1 Settings)

➤ **To create new authentication settings:**

1. Right-click the VPN client icon in your Windows system tray, and select **Configuration Panel**. The Configuration Panel screen displays.



VPN Configuration
Written by VpnConf 3.00
Last modification: 06-22-2011

VPN Client ready

Figure 112.

2. In the tree list pane of the Configuration Panel screen, right-click **VPN Configuration**, and select **New Phase 1**.

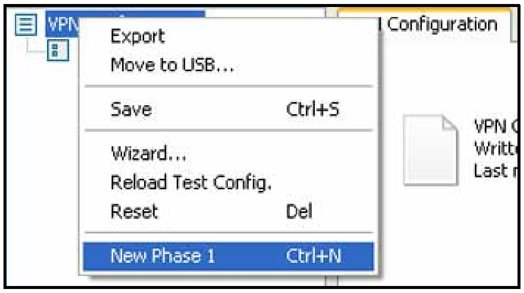
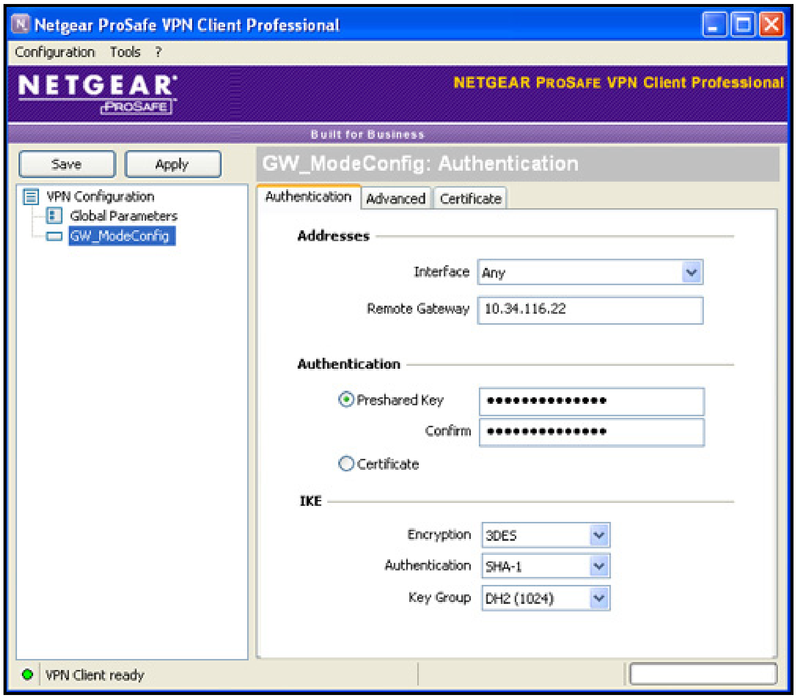


Figure 113.

3. Change the name of the authentication phase (the default is Gateway):
   - **a.** Right-click the authentication phase name.
   - **b.** Select **Rename**.
   - **c.** Type **GW_ModeConfig**.
   - **d.** Click anywhere in the tree list pane.

> ***Note:*** *This is the name for the authentication phase that is used only for the VPN client, not during IKE negotiation. You can view and change this name in the tree list pane. This name needs to be a unique name.*

The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default.



GW_ModeConfig: Authentication

Addresses

Interface: Any

Remote Gateway: 10.34.116.22

Authentication

● Preshared Key: ••••••••••••••

Confirm: ••••••••••••••

○ Certificate

IKE

Encryption: 3DES

Authentication: SHA-1

Key Group: DH2 (1024)

Figure 114.

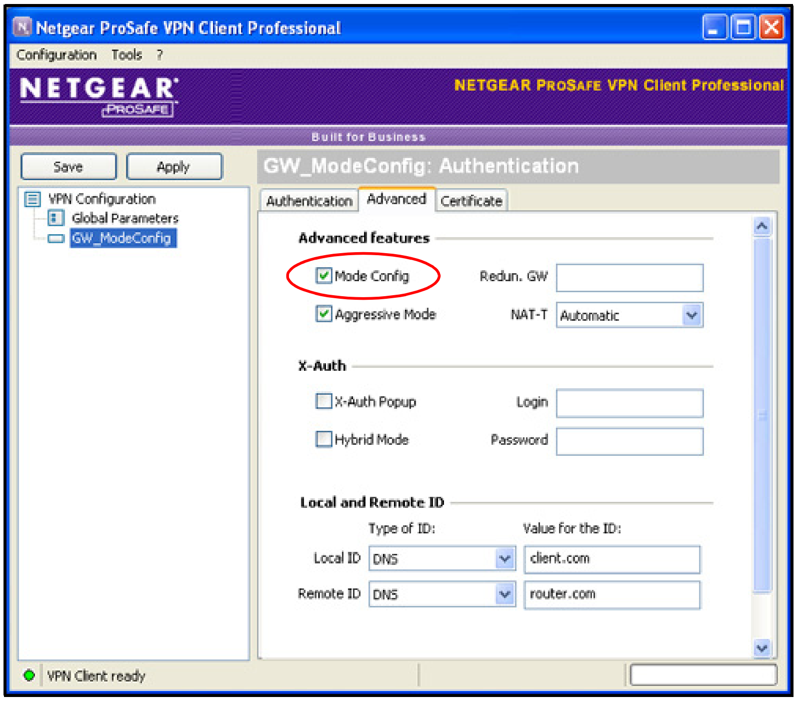
4. Specify the settings that are explained in the following table.

Table 45. VPN client authentication settings (Mode Config)

Setting	Description	
Interface	Select **Any** from the drop-down list.	
Remote Gateway	Enter the remote IP address or DNS name of the VPN firewall. For example, enter **10.34.116.22**.	
Preshared Key	Select the **Preshared Key** radio button. Enter the pre-shared key that you already specified on the VPN firewall. For example, enter **H8!spsf3#JYK2!**. Confirm the key in the Confirm field.	
IKE	Encryption	Select the **3DES** encryption algorithm from the drop-down list.
	Authentication	Select the **SHA1** authentication algorithm from the drop-down list.
	Key Group	Select the **DH2 (1024)** key group from the drop-down list. **Note:** On the VPN firewall, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).

5. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

6. Click the **Advanced** tab in the Authentication pane. The Advanced pane displays.



GW_ModeConfig: Authentication

Advanced features

☑ Mode Config

Redun. GW

☑ Aggressive Mode

NAT-T: Automatic

X-Auth

☐ X-Auth Popup

Login

☐ Hybrid Mode

Password

Local and Remote ID

	Type of ID:	Value for the ID:
Local ID	DNS	client.com
Remote ID	DNS	router.com

VPN Client ready

Figure 115.

7. Specify the settings that are explained in the following table.

Table 46. VPN client advanced authentication settings (Mode Config)

Setting	Description
Advanced features	
Mode Config	Select this check box to enable Mode Config.
Aggressive Mode	Select this check box to enable aggressive mode as the negotiation mode with the VPN firewall.
NAT-T	Select **Automatic** from the drop-down list to enable the VPN client and VPN firewall to negotiate NAT-T.
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the Local ID drop-down list because you specified FQDN in the VPN firewall configuration. As the value of the ID, enter **client.com** as the local ID for the VPN client. **Note:** The remote ID on the VPN firewall is the local ID on the VPN client.
Remote ID	As the type of ID, select **DNS** from the Remote ID drop-down list because you specified an FQDN in the VPN firewall configuration. As the value of the ID, enter **router.com** as the remote ID for the VPN firewall. **Note:** The local ID on the VPN firewall is the remote ID on the VPN client.

8. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Create the Mode Config IPSec Configuration (Phase 2 Settings)

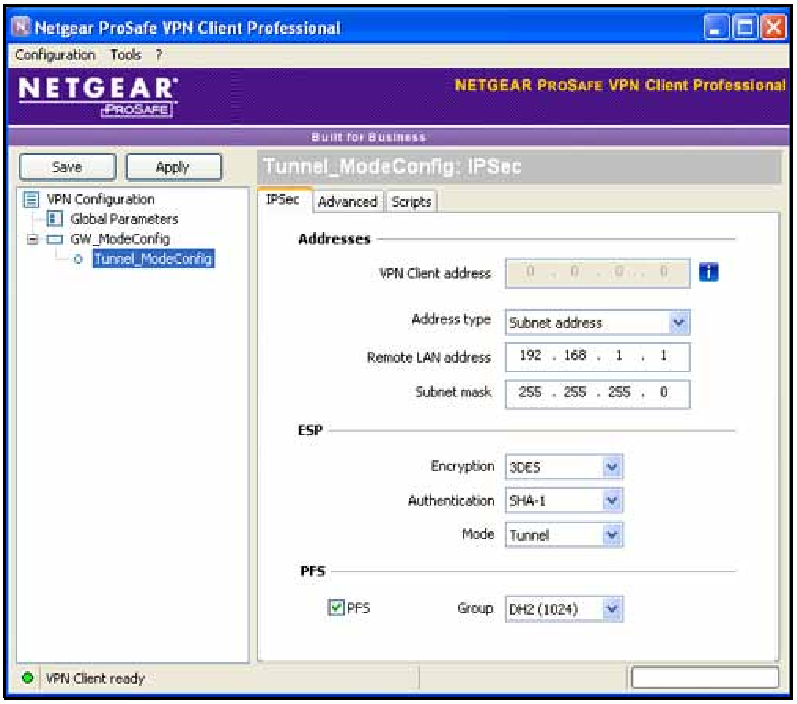
Note: On the VPN firewall, the IPSec configuration (phase 2 settings) is referred to as the IKE settings.

➢ **To create an IPSec configuration:**

1. In the tree list pane of the Configuration Panel screen, right-click the **GW_ModeConfig** authentication phase name, and then select **New Phase 2**.
2. Change the name of the IPSec configuration (the default is Tunnel):
   a. Right-click the IPSec configuration name.
   b. Select **Rename**.
   c. Type **Tunnel_ModeConfig**.
   d. Click anywhere in the tree list pane.

   Note: *This is the name for the IPSec configuration that is used only for the VPN client, not during IPSec negotiation. You can view and change this name in the tree list pane. This name needs to be a unique name.*

The IPSec pane displays in the Configuration Panel screen, with the IPSec tab selected by default.



Tunnel_ModeConfig: IPSec

Addresses

VPN Client address: 0 . 0 . 0 . 0

Address type: Subnet address

Remote LAN address: 192 . 168 . 1 . 1

Subnet mask: 255 . 255 . 255 . 0

ESP

Encryption: 3DES

Authentication: SHA-1

Mode: Tunnel

PFS

☑ PFS Group: DH2 (1024)

VPN Client ready

Figure 116.

3. Specify the settings that are explained in the following table.

Table 47. VPN client IPSec configuration settings (Mode Config)

Setting	Description
VPN Client address	This field is masked out because Mode Config is selected. After an IPSec connection is established, the IP address that is issued by the VPN firewall displays in this field (see *Figure 121* on page 192).
Address Type	Select **Subnet address** from the drop-down list.
Remote host address	The address that you need to enter depends on whether or not you have specified a LAN IP network address in the Local IP Address field on the Add Mode Config Record screen of the VPN firewall: • If you left the Local IP Address field blank, enter the VPN firewall’s default LAN IP address as the remote host address that opens the VPN tunnel. For example, enter **192.168.1.1**. • If you specified a LAN IP network address in the Local IP Address field, enter the address that you specified as the remote host address that opens the VPN tunnel.
Subnet Mask	Enter **255.255.255.0** as the remote subnet mask of the VPN firewall that opens the VPN tunnel. This is the LAN IP subnet mask that you specified in the Local Subnet Mask field on the Add Mode Config Record screen of the VPN firewall. If you left the Local Subnet Mask field blank, enter the VPN firewall’s default IP subnet mask.

Table 47. VPN client IPSec configuration settings (Mode Config) (continued)

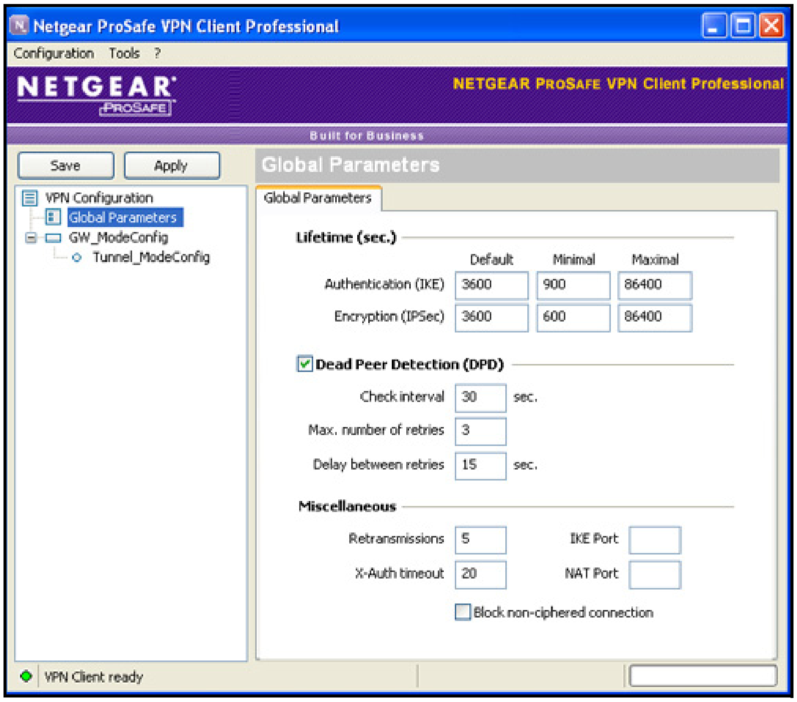
Setting	Description	
ESP	Encryption	Select **3DES** as the encryption algorithm from the drop-down list.
	Authentication	Select **SHA-1** as the authentication algorithm from the drop-down list.
	Mode	Select **Tunnel** as the encapsulation mode from the drop-down list.
PFS and Group	Select the **PFS** check box, and then select the **DH2 (1024)** key group from the drop-down list. **Note:** On the VPN firewall, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).	

4. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

Configure the Mode Config Global Parameters

➤ **To specify the global parameters:**

1. Click **Global Parameters** in the left column of the Configuration Panel screen. The Global Parameters pane displays in the Configuration Panel screen.



Lifetime (sec.)

	Default	Minimal	Maximal
Authentication (IKE)	3600	900	86400
Encryption (IPSec)	3600	600	86400

☑ Dead Peer Detection (DPD)

Check interval 30 sec.

Max. number of retries 3

Delay between retries 15 sec.

Miscellaneous

Retransmissions 5

IKE Port

X-Auth timeout 20

NAT Port

☐ Block non-ciphered connection

VPN Client ready

Figure 117.

2. Specify the following default lifetimes in seconds to match the configuration on the VPN firewall:
   - **Authentication (IKE)**, **Default**. Enter **3600** seconds.
   - **Encryption (IPSec)**, **Default**. Enter **3600** seconds.
3. Select the **Dead Peer Detection (DPD)** check box, and configure the following DPD settings to match the configuration on the VPN firewall:
   - **Check Interval**. Enter **30** seconds.
   - **Max. number of entries**. Enter **3** retries.
   - **Delay between entries**. Leave the default delay setting of 15 seconds.
4. Click **Apply** to use the new settings immediately, and click **Save** to keep the settings for future use.

The Mode Config configuration of the VPN client is now complete.

Test the Mode Config Connection

➢ **To test the Mode Config connection from the VPN client to the VPN firewall:**

1. Right-click the system tray icon, and click **Open tunnel 'Tunnel_ModeConfig'**.

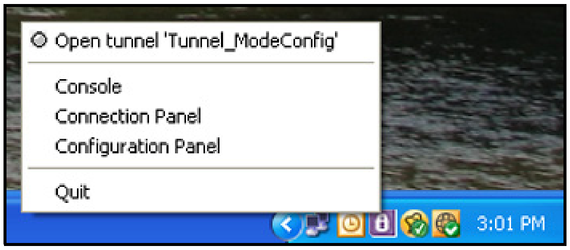
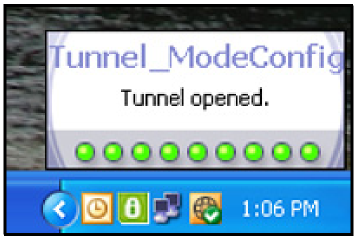


Figure 118.

When the tunnel opens successfully, the *Tunnel opened* message displays above the system tray, and the VPN client displays a green icon in the system tray.

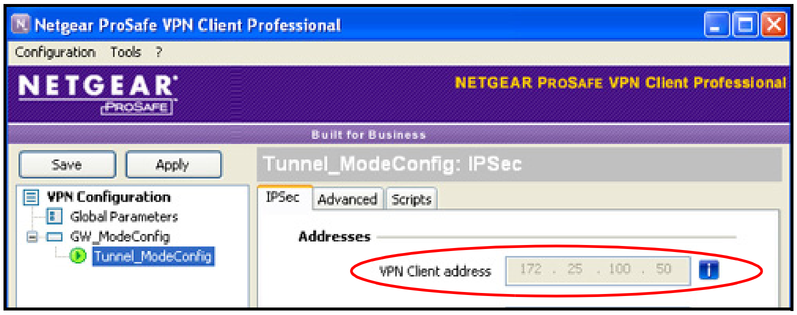


Tunnel_ModeConfig

Tunnel opened.

Figure 119.

2. Verify that the VPN firewall issued an IP address to the VPN client. This IP address displays in the VPN Client address field on the IPSec pane of the VPN client. (The following figure shows the upper part of the IPSec pane only.)



VPN Client address 172 . 25 . 100 . 50

Figure 120.

3. From the client PC, ping a computer on the VPN firewall LAN.

Modify or Delete a Mode Config Record

➢ **To edit a Mode Config record:**

1. On the Mode Config screen (see *Figure 109* on page 177), click the **Edit** table button in the Action column for the record that you want to modify. The Edit Mode Config Record screen displays. This screen is identical to the Add Mode Config Record screen (see *Figure 110* on page 178).
2. Modify the settings as explained in *Table 43* on page 178.
3. Click **Apply** to save your settings.

➢ **To delete one or more Mode Config records:**

1. On the Mode Config screen (see *Figure 109* on page 177), select the check box to the left of the record that you want to delete, or click the **Select All** table button to select all records.
2. Click the **Delete** table button.

Configure Keep-alives and Dead Peer Detection

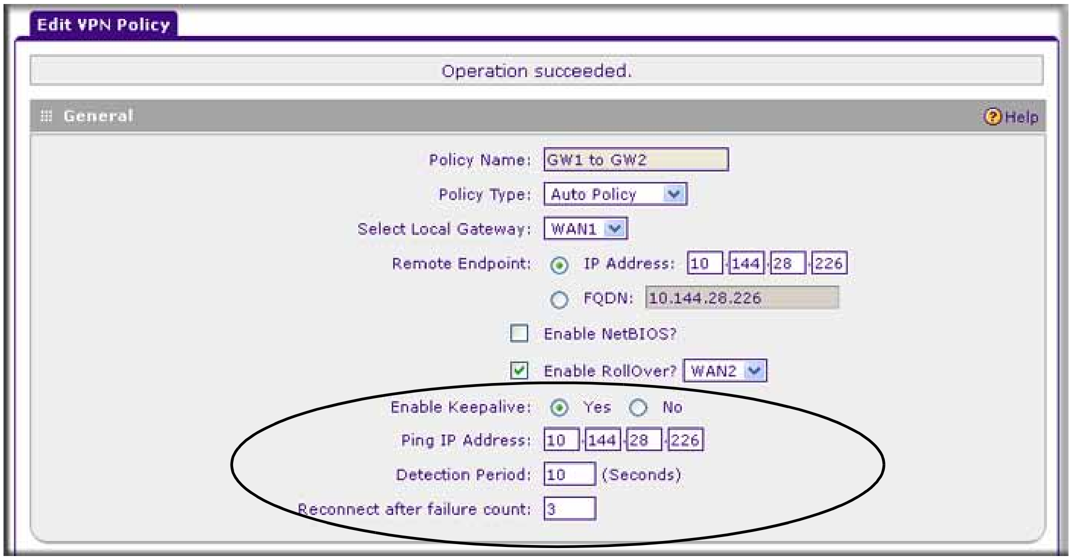
In some cases, you might not want a VPN tunnel to be disconnected when traffic is idle, for example, when client-server applications over the tunnel cannot tolerate the tunnel establishment time. If you require a VPN tunnel to remain connected, you can use the keep-alive and Dead Peer Detection (DPD) features to prevent the tunnel from being disconnected and to force a reconnection if the tunnel disconnects for any reason.

For DPD to function, the peer VPN device on the other end of the tunnel should also support DPD. Keep-alive, though less reliable than DPD, does not require any support from the peer device.

Configure Keep-alives

The keep-alive feature maintains the IPSec SA by sending periodic ping requests to a host across the tunnel and monitoring the replies. To configure the keep-alive feature on a configured VPN policy:

1. Select **VPN > IPSec VPN > VPN Policies**. The VPN Policies screen displays (see *Figure 106* on page 166).
2. In the List of VPN Policies table, click the **Edit** table button to the right of the VPN policy that you want to edit. The Edit VPN Policy screen displays. (The following figure shows only the top part of the screen with the General section.)



Edit VPN Policy

Operation succeeded.

General

Policy Name: GW1 to GW2

Policy Type: Auto Policy

Select Local Gateway: WAN1

Remote Endpoint: ● IP Address: 10 . 144 . 28 . 226

○ FQDN: 10.144.28.226

□ Enable NetBIOS?

☑ Enable RollOver? WAN2

Enable Keepalive: ● Yes ○ No

Ping IP Address: 10 . 144 . 28 . 226

Detection Period: 10 (Seconds)

Reconnect after failure count: 3

Figure 121.

3. Enter the settings as explained in the following table:

Table 48. Keep-alive settings

Setting	Description	
General		
Enable Keepalive	Select a radio button to specify if keep-alive is enabled: • **Yes**. This feature is enabled. Periodically, the VPN firewall sends keep-alive requests (ping packets) to the remote endpoint to keep the tunnel alive. You need to enter the ping IP address, detection period, and the maximum number of keep-alive requests that the VPN firewall sends (see below). • **No**. This feature is disabled. This is the default setting.	
	Ping IP Address	The IP address that the VPN firewall pings. The address needs to be of a host that can respond to ICMP ping requests.

Table 48. Keep-alive settings (continued)

Setting	Description	
Enable Keepalive (continued)	Detection Period	The period in seconds between the keep-alive requests. The default setting is 10 seconds.
	Reconnect after failure count	The maximum number of keep-alive requests before the VPN firewall tears down the connection and then attempts to reconnect to the remote endpoint. The default is 3 keep-alive requests.

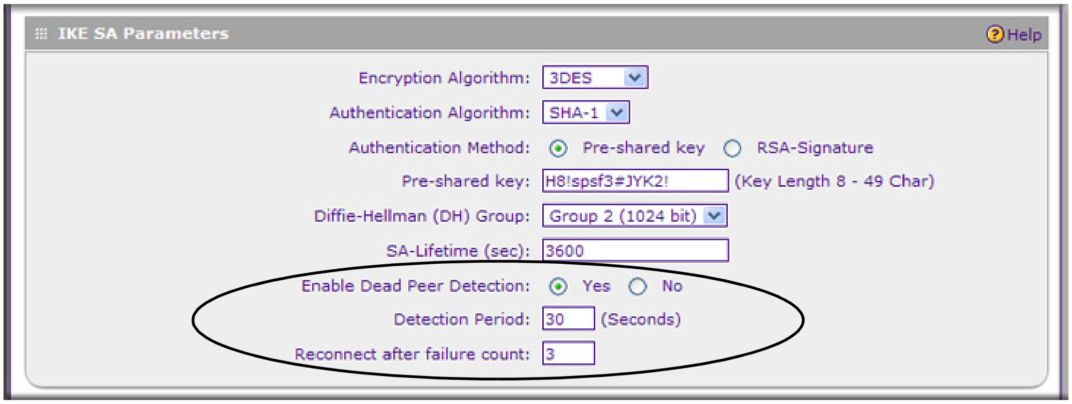
4. Click **Apply** to save your settings.

Configure Dead Peer Detection

The Dead Peer Detection (DPD) feature maintains the IKE SA by exchanging periodic messages with the remote VPN peer.

➤ **To configure DPD on a configured IKE policy:**

1. Select **VPN > IPSec VPN**. The IPSec VPN submenu tabs display, with the IKE Policies screen in view (see *Figure 104* on page 160).
2. In the List of IKE Policies table, click the **Edit** table button to the right of the IKE policy that you want to edit. The Edit IKE Policy screen displays. (The following figure shows only the IKE SA Parameters section of the screen.)



IKE SA Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

Authentication Method: ● Pre-shared key ○ RSA-Signature

Pre-shared key: H8!spsf3#JYK2! (Key Length 8 - 49 Char)

Diffie-Hellman (DH) Group: Group 2 (1024 bit)

SA-Lifetime (sec): 3600

Enable Dead Peer Detection: ● Yes ○ No

Detection Period: 30 (Seconds)

Reconnect after failure count: 3

Figure 122.

3. In the IKE SA Parameters section of the screen, locate the DPD fields, and complete the settings as explained the following table:

Table 49. Dead Peer Detection settings

Setting	Description	
IKE SA Parameters		
Enable Dead Peer Detection	Select the **Yes** radio button to enable DPD. When the VPN firewall detects an IKE connection failure, it deletes the IPSec and IKE SA and forces a reestablishment of the connection. You need to specify the detection period in the **Detection Period** field and the maximum number of times that the VPN firewall attempts to reconnect in the **Reconnect after failure count** field.	
	Detection Period	The period in seconds between consecutive DPD R-U-THERE messages, which are sent only when the IPSec traffic is idle. The default setting is 10 seconds.
	Reconnect after failure count	The maximum number of DPD failures before the VPN firewall tears down the connection and then attempts to reconnect to the peer. The default is 3 failures.

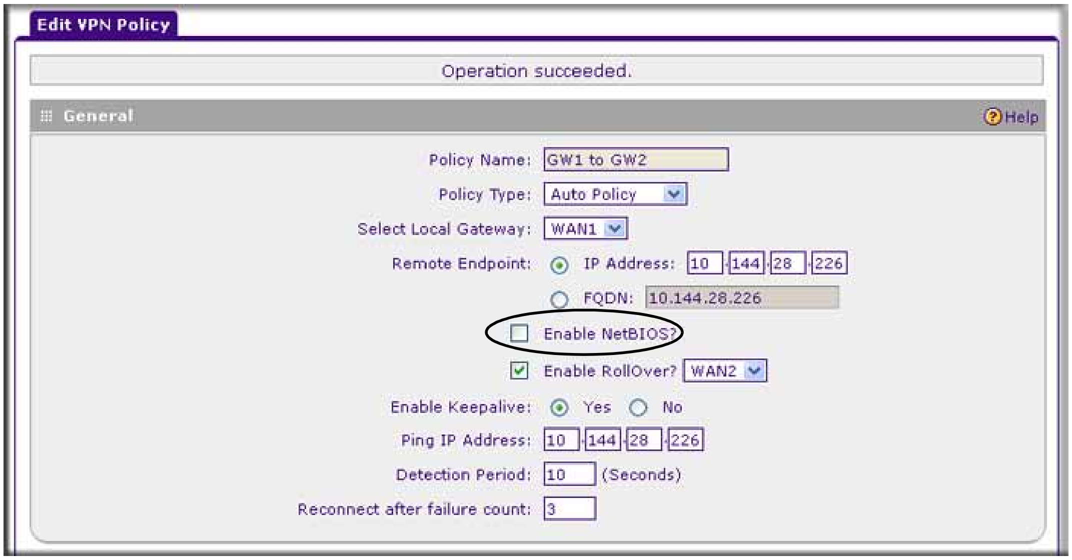
4. Click **Apply** to save your settings.

Configure NetBIOS Bridging with IPSec VPN

Windows networks use the Network Basic Input/Output System (NetBIOS) for several basic network services such as naming and neighborhood device discovery. Because VPN routers do not normally pass NetBIOS traffic, these network services do not function for hosts on opposite ends of a VPN connection. To solve this problem, you can configure the VPN firewall to bridge NetBIOS traffic over the VPN tunnel.

➢ **To enable NetBIOS bridging on a configured VPN tunnel:**

1. Select **VPN > IPSec VPN > VPN Policies**. The VPN Policies screen displays (see *Figure 106* on page 166).
2. In the List of VPN Policies table, click the **Edit** table button to the right of the VPN policy that you want to edit. The Edit VPN Policy screen displays. (The following figure shows only the top part of the screen with the General section.)



Edit VPN Policy

Operation succeeded.

General

Policy Name: GW1 to GW2

Policy Type: Auto Policy

Select Local Gateway: WAN1

Remote Endpoint: ● IP Address: 10 . 144 . 28 . 226

○ FQDN: 10.144.28.226

□ Enable NetBIOS?

☑ Enable RollOver? WAN2

Enable Keepalive: ● Yes ○ No

Ping IP Address: 10 . 144 . 28 . 226

Detection Period: 10 (Seconds)

Reconnect after failure count: 3

Figure 123.

3. Select the **Enable NetBIOS** check box.
4. Click **Apply** to save your settings.

Virtual Private Networking Using SSL Connections

6

The VPN firewall provides a hardware-based SSL VPN solution designed specifically to provide remote access for mobile users to their corporate resources, bypassing the need for a preinstalled VPN client on their computers. Using the familiar Secure Sockets Layer (SSL) protocol, commonly used for e-commerce transactions, the VPN firewall can authenticate itself to an SSL-enabled client, such as a standard web browser. Once the authentication and negotiation of encryption information are completed, the server and client can establish an encrypted connection. With support for up to 50 dedicated SSL VPN tunnels, the VPN firewall allows users to easily access the remote network for a customizable, secure, user portal experience from virtually any available platform.

This chapter contains the following sections:

SSL VPN Portal Options

The VPN firewall's SSL VPN portal can provide two levels of SSL service to the remote user:

- **SSL VPN tunnel**. The VPN firewall can provide the full network connectivity of a VPN tunnel using the remote user's browser instead of a traditional IPSec VPN client.

  The SSL capability of the user's browser provides authentication and encryption, establishing a secure connection to the VPN firewall. Upon successful connection, an ActiveX-based SSL VPN client is downloaded to the remote PC to allow the remote user to virtually join the corporate network.

The SSL VPN client provides a point-to-point (PPP) connection between the client and the VPN firewall, and a virtual network interface is created on the user's PC. The VPN firewall assigns the PC an IP address and DNS server IP addresses, allowing the remote PC to access network resources in the same manner as if it were connected directly to the corporate network, subject to any policy restrictions that you configure.

- **SSL port forwarding**. Like an SSL VPN tunnel, port forwarding is a web-based client that is installed transparently and then creates a virtual, encrypted tunnel to the remote network. However, port forwarding differs from an SSL VPN tunnel in several ways:
  - Port forwarding supports only TCP connections, not UDP connections or connections using other IP protocols.
  - Port forwarding detects and reroutes individual data streams on the user's PC to the port-forwarding connection rather than opening up a full tunnel to the corporate network.
  - Port forwarding offers more fine-grained management than an SSL VPN tunnel. You define individual applications and resources that are available to remote users.

The SSL VPN portal can present the remote user with one or both of these SSL service levels, depending on how you set up the configuration.

Overview of the SSL Configuration Process

➤ **To configure and activate SSL connections, perform the following six basic steps in the order that they are presented:**

1. Edit the existing SSL portal or create a new one (see *Create the Portal Layout* on page 198).

   When remote users log in to the VPN firewall, they see a portal page that you can customize to present the resources and functions that you choose to make available.

2. Create authentication domains, user groups, and user accounts (see *Configure Domains, Groups, and Users* on page 202).

   a. Create one or more authentication domains for authentication of SSL VPN users. When remote users log in to the VPN firewall, they need to specify a domain to which their login account belongs.

      The domain determines the authentication method that is used and the portal layout that is presented, which in turn determines the network resources to which the users are granted access. Because you need to assign a portal layout when creating a domain, the domain is created after you have created the portal layout.

   b. Create one or more groups for your SSL VPN users.

      When you define the SSL VPN policies that determine network resource access for your SSL VPN users, you can define global policies, group policies, or individual policies. Because you need to assign an authentication domain when creating a group, the group is created after you have created the domain.

   c. Create one or more SSL VPN user accounts.

Because you need to assign a group when creating a SSL VPN user account, the user account is created after you have created the group.

3. For port forwarding, define the servers and services (*Configure Applications for Port Forwarding* on page 202).

   Create a list of servers and services that can be made available through user, group, or global policies. You can also associate fully qualified domain names (FQDNs) with these servers. The VPN firewall resolves the names to the servers using the list you have created.

4. For SSL VPN tunnel service, configure the virtual network adapter (see *Configure the SSL VPN Client* on page 205).

   For the SSL VPN tunnel option, the VPN firewall creates a virtual network adapter on the remote PC that then functions as if it were on the local network. Configure the portal's SSL VPN client to define a pool of local IP addresses to be issued to remote clients, as well as DNS addresses. Declare static routes or grant full access to the local network, subject to additional policies.

5. To simplify policies, define network resource objects (see *Use Network Resource Objects to Simplify Policies* on page 208).

   Network resource objects are groups of IP addresses, IP address ranges, and services. By defining resource objects, you can more quickly create and configure network policies.

6. Configure the SSL VPN policies (see *Configure User, Group, and Global Policies* on page 210).

   Policies determine access to network resources and addresses for individual users, groups, or everyone.

Create the Portal Layout

The Portal Layouts screen that you can access from the SSL VPN menu allows you to create a custom page that remote users see when they log in to the portal. Because the page is completely customizable, it provides an ideal way to communicate remote access instructions, support information, technical contact information, or VPN-related news updates to remote users. The page is also well-suited as a starting page for restricted users; if mobile users or business partners are permitted to access only a few resources, the page that you create presents only the resources that are relevant to these users.

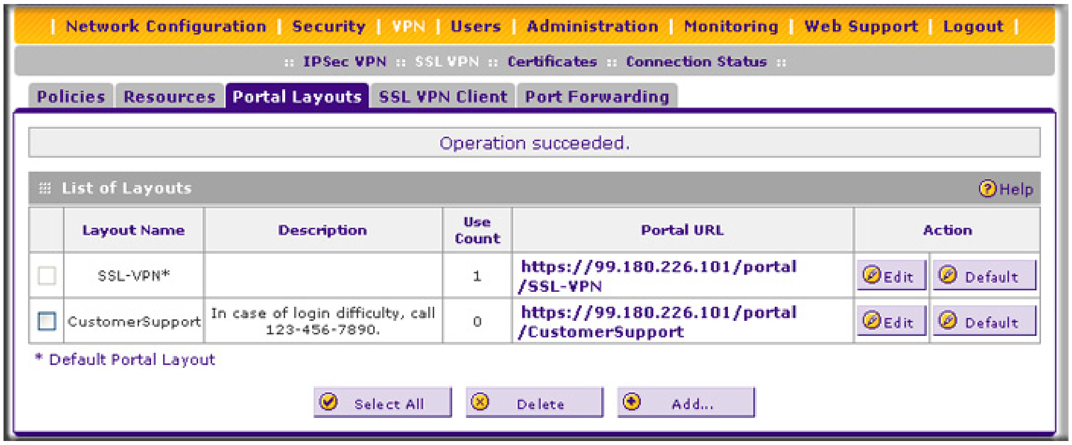
You apply portal layouts by selecting one from the available portal layouts in the configuration of a domain. When you have completed your portal layout, you can apply the portal layout to one or more authentication domains (see *Configure Domains* on page 219). You can also make the new portal the default portal for the SSL VPN gateway by selecting the default radio button adjacent to the portal layout name.

Note: The VPN firewall’s default portal address is **https://<*IP_Address*>/portal/SSL-VPN**.
The default domain **geardomain** is attached to the SSL-VPN portal.

You can define individual layouts for the SSL VPN portal. The layout configuration includes the menu layout, theme, portal pages to display, and web cache control options. The default portal layout is the SSL-VPN portal. You can add additional portal layouts. You can also make any portal the default portal for the VPN firewall by clicking the **Default** button in the Action column of the List of Layouts table, to the right of the desired portal layout.

➢ To create a new SSL VPN portal layout:

1. Select **VPN > SSL VPN > Portal Layouts**. The Portal Layout screen displays. (The following figure shows layouts in the List of Layouts table as an example. (The IP address that is shown in this figure do not relate to other figures and examples in this manual.)


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
:: IPSec VPN :: SSL VPN :: Certificates :: Connection Status ::
Policies
Resources
Portal Layouts
SSL VPN Client
Port Forwarding
List of Layouts
Help
* Default Portal Layout
Select All
Delete
Add...

Operation succeeded.

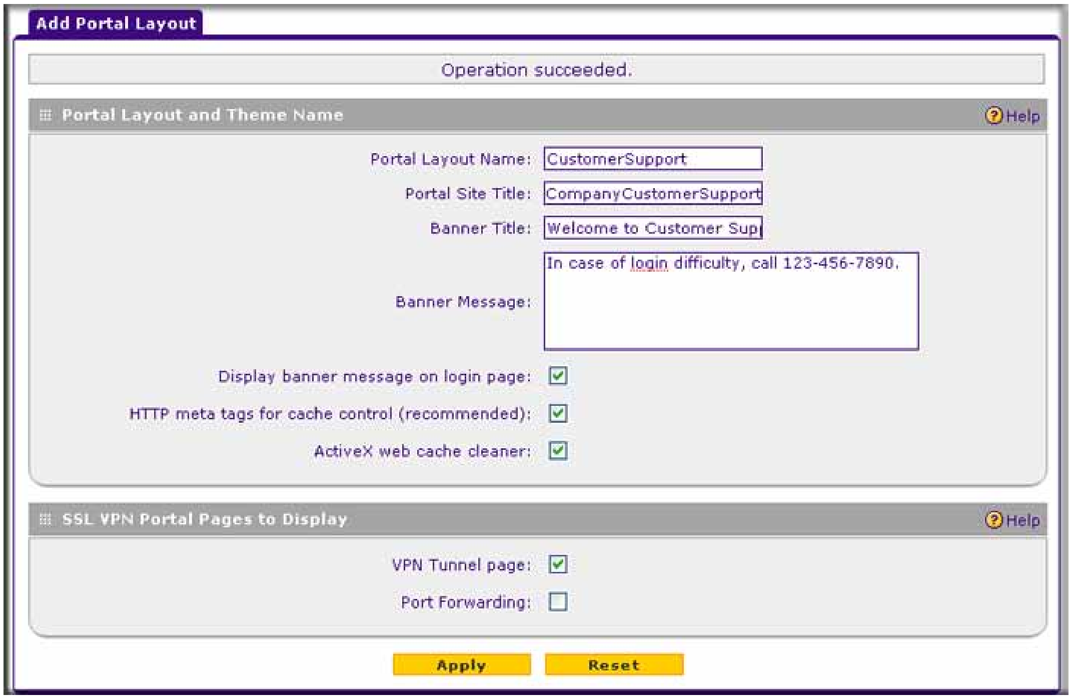
	Layout Name	Description	Use Count	Portal URL	Action
□	SSL-VPN*		1	https://99.180.226.101/portal/SSL-VPN	Edit Default
□	CustomerSupport	In case of login difficulty, call 123-456-7890.	0	https://99.180.226.101/portal/CustomerSupport	Edit Default

Figure 124.

The List of Layouts table displays the following fields:

- **Layout Name**. The descriptive name of the portal.
- **Description**. The banner message that is displayed at the top of the portal (see *Figure 132* on page 217).
- **Use Count**. The number of remote users that are currently using the portal.
- **Portal URL**. The URL at which the portal can be accessed.
- **Action**. The table buttons that allow you to edit the portal layout or set it as the default.

2. Under the List of Layouts table, click the **Add** table button. The Add Portal Layout screen displays. (The following figure shows an example.)



Portal Layout Name: CustomerSupport

Portal Site Title: CompanyCustomerSupport

Banner Title: Welcome to Customer Sup

Banner Message: In case of login difficulty, call 123-456-7890.

Display banner message on login page: ☑

HTTP meta tags for cache control (recommended): ☑

ActiveX web cache cleaner: ☑

VPN Tunnel page: ☑

Port Forwarding: □

Figure 125.

3. Complete the settings as explained the following table:

Table 50. Add Portal Layout screen settings

Setting	Description
Portal Layout and Theme Name	
Portal Layout Name	A descriptive name for the portal layout. This name is part of the path of the SSL VPN portal URL. **Note:** Custom portals are accessed at a different URL than the default portal. For example, if your SSL VPN portal is hosted at https://vpn.company.com, and you create a portal layout named CustomerSupport, then users access the sub-site at https://vpn.company.com/portal/CustomerSupport. **Note:** Only alphanumeric characters, hyphens (-), and underscores (_) are accepted in the Portal Layout Name field. If you enter other types of characters or spaces, the layout name is truncated before the first nonalphanumeric character. **Note:** Unlike most other URLs, this name is case-sensitive.
Portal Site Title	The title that appears at the top of the user’s web browser window, for example, Company Customer Support.
Banner Title	The banner title of a banner message that users see before they log in to the portal, for example, Welcome to Customer Support. **Note:** For an example, see *Figure 132* on page 217. The banner title text is displayed in the orange header bar.

Table 50. Add Portal Layout screen settings (continued)

Setting	Description
Banner Message	The text of a banner message that users see before they log in to the portal, for example, In case of login difficulty, call 123-456-7890. Enter a plain text message or include HTML and JavaScript tags. The maximum length of the login page message is 4096 characters. **Note:** For an example, see *Figure 132* on page 217. The banner message text is displayed in the gray header bar.
Display banner message on login page	Select this check box to show the banner title and banner message text on the login screen as shown in *Figure 132* on page 217.

HTTP meta tags for cache control (recommended)	Select this check box to apply HTTP meta tag cache control directives to this portal layout. Cache control directives include:
	`<meta http-equiv=”pragma” content=”no-cache”>`
	`<meta http-equiv=”cache-control” content=”no-cache”>`
	`<meta http-equiv=”cache-control” content=”must-revalidate”>`
	Note: NETGEAR strongly recommends enabling HTTP meta tags for security reasons and to prevent out-of-date web pages, themes, and data being stored in a user’s web browser cache.

ActiveX web cache cleaner	Select this check box to enable ActiveX cache control to be loaded when users log in to the SSL VPN portal. The web cache cleaner prompts the user to delete all temporary Internet files, cookies, and browser history when the user logs out or closes the web browser window. The ActiveX web cache control is ignored by web browsers that do not support ActiveX.
SSL VPN Portal Pages to Display	
VPN Tunnel page	Select this check box to provide full network connectivity.
Port Forwarding	Select this check box to provide access to specific defined network services. (See *Configure Applications for Port Forwarding* on page 202.) **Note:** Any pages that are not selected are not visible from the SSL VPN portal; however, users can still access the hidden pages unless you create SSL VPN access policies to prevent access to these pages.

4. Click **Apply** to save your settings. The new portal layout is added to the List of Layouts table. For information about how to display the new portal layout, see *Access the SSL Portal Login Screen* on page 216.

➢ To edit a portal layout:

1. On the Portal Layouts screen (see *Figure 124* on page 199), click the **Edit** button in the Action column for the portal layout that you want to modify. The Edit Portal Layout screen displays. This screen is identical to the Add Portal Layout screen (see the previous figure).
2. Modify the settings as explained in the previous table.
3. Click **Apply** to save your settings.

➢ **To delete one or more portal layouts:**

1. On the Portal Layouts screen (see *Figure 124* on page 199), select the check box to the left of the portal layout that you want to delete, or click the **Select All** table button to select all layouts. (You cannot delete the SSL-VPN default portal layout.)
2. Click the **Delete** table button.

Configure Domains, Groups, and Users

Remote users connecting to the VPN firewall through an SSL VPN portal need to be authenticated before they are being granted access to the network. The login window that is presented to the user requires three items: a user name, a password, and a domain selection. The domain determines both the authentication method and the portal layout that are used.

You need to create name and password accounts for the SSL VPN users. When you create a user account, you need to specify a group. Groups are used to simplify the application of access policies. When you create a group, you need to specify a domain. Therefore, you should create any domains first, then groups, and then user accounts.

To configure domains, groups, and users, see *Configure VPN Authentication Domains, Groups, and Users* on page 219.

Configure Applications for Port Forwarding

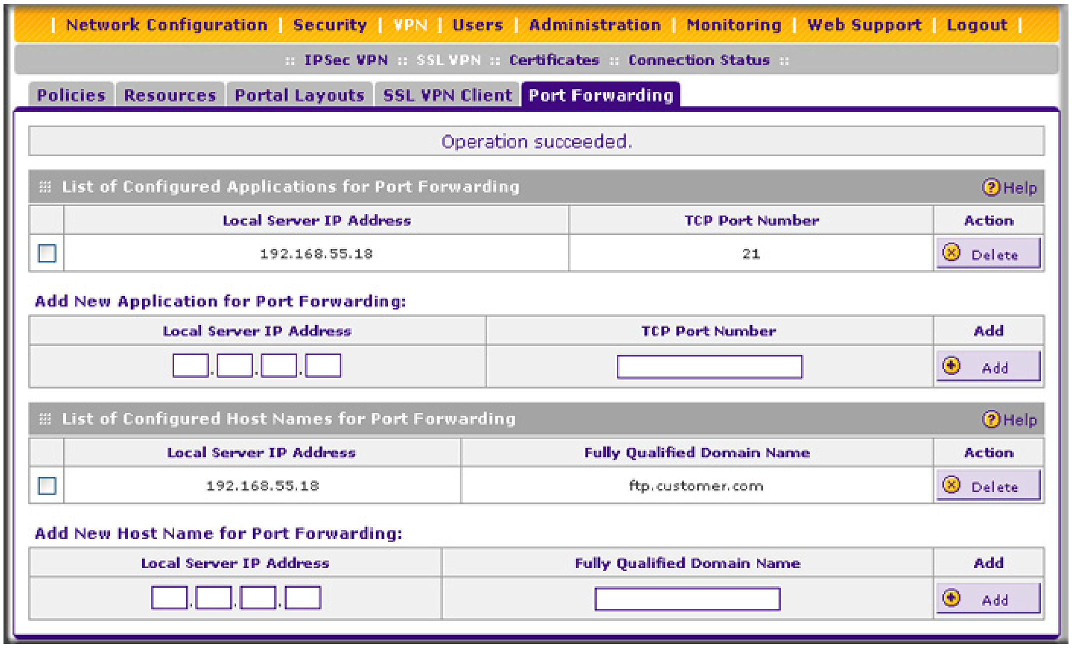
Port forwarding provides access to specific defined network services. To define these services, you need to specify the internal server addresses and port numbers for TCP applications that are intercepted by the port-forwarding client on the user’s PC. This client reroutes the traffic to the VPN firewall.

Add Servers and Port Numbers

To configure port forwarding, you need to define the IP addresses of the internal servers and the port number for TCP applications that are available to remote users.

➢ **To add a server and a port number:**

1. Select **VPN > SSL VPN > Port Forwarding**. The Port Forwarding screen displays. (The following figure shows an example.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: Certificates :: Connection Status ::
Policies
Resources
Portal Layouts
SSL VPN Client
Port Forwarding
Help
Delete
Add

Operation succeeded.

List of Configured Applications for Port Forwarding

	Local Server IP Address	TCP Port Number	Action
□	192.168.55.18	21	Delete

Add New Application for Port Forwarding:

Local Server IP Address	TCP Port Number	Add
. . .		Add

List of Configured Host Names for Port Forwarding

	Local Server IP Address	Fully Qualified Domain Name	Action
□	192.168.55.18	ftp.customer.com	Delete

Add New Host Name for Port Forwarding:

Local Server IP Address	Fully Qualified Domain Name	Add
. . .		Add

Figure 126.

2. In the Add New Application for Port Forwarding section of the screen, specify information in the following fields:
   - **IP Address**. The IP address of an internal server or host computer that a remote user has access to.
   - **TCP Port**. The TCP port number of the application that is accessed through the SSL VPN tunnel. The following table lists some commonly used TCP applications and port numbers:

Table 51. Port-forwarding applications/TCP port numbers

TCP application	Port number
FTP data (usually not needed)	20
FTP Control Protocol	21
SSH	22[a]
Telnet	23[a]
SMTP (send mail)	25
HTTP (web)	80
POP3 (receive mail)	110
NTP (Network Time Protocol)	123
Citrix	1494

Table 51. Port-forwarding applications/TCP port numbers (continued)

TCP application	Port number
Terminal Services	3389
VNC (virtual network computing)	5900 or 5800

a. Users can specify the port number together with the host name or IP address.

3. Click the **Add** table button. The new application entry is added to the List of Configured Applications for Port Forwarding table. Remote users can now securely access network applications once they have logged in to the SSL VPN portal and launched port forwarding.

➤ **To delete an application from the List of Configured Applications for Port Forwarding table:**

Select the check box to the left of the application that you want to delete, and then click the **Delete** table button in the Action column.

Add a New Host Name

After you have configured port forwarding by defining the IP addresses of the internal servers and the port number for TCP applications that are available to remote users, you then can also specify host-name-to-IP-address resolution for the network servers as a convenience for users. Host name resolution allows users to access TCP applications at familiar addresses such as mail.*example*.com or ftp.*customer*.com rather than by IP addresses.

➤ **To add servers and host names for client name resolution:**

1. Select **VPN > SSL VPN > Port Forwarding**. The Port Forwarding screen displays (see *Figure 126* on page 203).
2. In the Add New Host Name for Port Forwarding section of the screen, specify information in the following fields:
   - **Local Server IP Address**. The IP address of an internal server or host computer that you want to name.
   - **Fully Qualified Domain Name**. The full server name.

Note: If the server or host computer that you want to name does not appear in the List of Configured Applications for Port Forwarding table, you need to add it before you can rename it.

3. Click the **Add** table button. The new application entry is added to the List of Configured Host Names for Port Forwarding table.

To delete a name from the List of Configured Host Names for Port Forwarding table, select the check box to the left of the name that you want to delete, and then click the **Delete** table button in the Action column.

Configure the SSL VPN Client

The SSL VPN client on the VPN firewall assigns IP addresses to remote VPN tunnel clients. Because the VPN tunnel connection is a point-to-point connection, you can assign IP addresses from the local subnet to the remote VPN tunnel clients.

The following are some additional considerations:

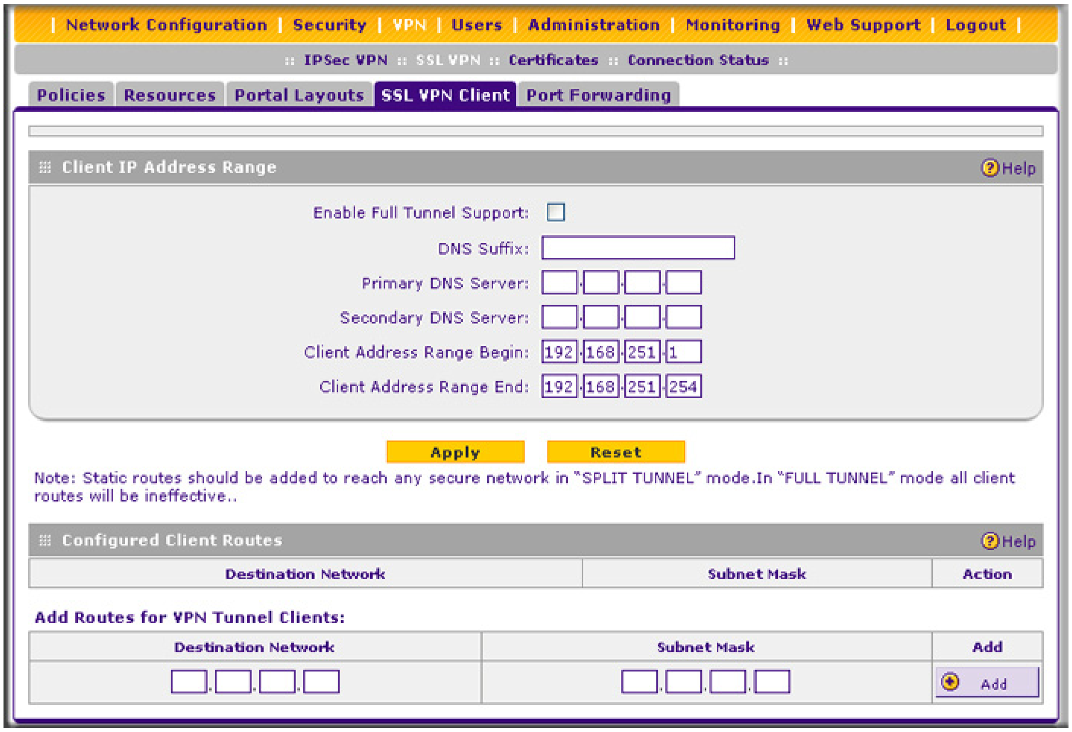
- So that the virtual (PPP) interface address of a VPN tunnel client does not conflict with addresses on the local network, configure an IP address range that does not directly overlap with addresses on your local network. For example, if 192.168.1.1 through 192.168.1.100 are currently assigned to devices on the local network, then start the client address range at 192.168.1.101 or choose an entirely different subnet altogether.
- The VPN tunnel client cannot contact a server on the local network if the VPN tunnel client's Ethernet interface shares the same IP address as the server or the VPN firewall (for example, if your PC has a network interface IP address of 10.0.0.45, then you cannot contact a server on the remote network that also has the IP address 10.0.0.45).
- Select whether you want to enable full tunnel or split tunnel support based on your bandwidth:
  - A full tunnel sends all of the client's traffic across the VPN tunnel.
  - A split tunnel sends only traffic that is destined for the local network based on the specified client routes. All other traffic is sent to the Internet. A split tunnel allows you to manage bandwidth by reserving the VPN tunnel for local traffic only.
- If you enable split tunnel support and you assign an entirely different subnet to the VPN tunnel clients from the subnet that is used by the local network, you need to add a client route to ensure that a VPN tunnel client connects to the local network over the VPN tunnel.

Configure the Client IP Address Range

First determine the address range to be assigned to VPN tunnel clients, then define the address range.

➢ **To define the client IP address range:**

1. Select **VPN > SSL VPN > SSL VPN Client**. The SSL VPN Client screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: Certificates :: Connection Status ::
Policies
Resources
Portal Layouts
SSL VPN Client
Port Forwarding
Help
Apply
Reset
Help
Add

Client IP Address Range

Enable Full Tunnel Support: □

DNS Suffix:

Primary DNS Server:

Secondary DNS Server:

Client Address Range Begin: 192.168.251.1

Client Address Range End: 192.168.251.254

Note: Static routes should be added to reach any secure network in "SPLIT TUNNEL" mode.In "FULL TUNNEL" mode all client routes will be ineffective..

Configured Client Routes

Destination Network	Subnet Mask	Action

Add Routes for VPN Tunnel Clients:

Destination Network	Subnet Mask	Add
. . .	. . .	Add

Figure 127.

2. Complete the settings as explained the following table:

Table 52. SSL VPN client IP address range settings

Setting	Description
Client IP Address Range	
Enable Full Tunnel Support	Select this check box to enable full tunnel support. If you leave this check box cleared (which is the default setting), split-tunnel support is enabled, and you need to add client routes (see *Add Routes for VPN Tunnel Clients* on page 207). **Note:** When full tunnel support is enabled, client routes are not operable.
DNS Suffix	A DNS suffix to be appended to incomplete DNS search strings. This is optional.
Primary DNS Server	The IP address of the primary DNS server that is assigned to the VPN tunnel clients. This is optional. **Note:** If you do not assign a DNS server, the DNS settings remain unchanged in the VPN client after a VPN tunnel has been established.
Secondary DNS Server	The IP address of the secondary DNS server that is assigned to the VPN tunnel clients. This is optional.

Table 52. SSL VPN client IP address range settings (continued)

Setting	Description
Client Address Range Begin	The first IP address of the IP address range that you want to assign to the VPN tunnel clients.
Client Address Range End	The last IP address of the IP address range that you want to assign to the VPN tunnel clients.

3. Click **Apply** to save your settings. VPN tunnel clients are now able to connect to the VPN firewall and receive a virtual IP address in the client address range.

Add Routes for VPN Tunnel Clients

The VPN tunnel clients assume that the following networks are located across the VPN-over-SSL tunnel:

- The subnet that contains the client IP address (that is, PPP interface), as determined by the class of the address (Class A, B, or C).
- Subnets that are specified in the Configured Client Routes table on the SSL VPN Client screen.

If the assigned client IP address range is in a different subnet from the local network, or if the local network has multiple subnets, or if you select split mode tunnel operation, you need to define client routes.

➤ **To add an SSL VPN tunnel client route:**

1. Select **VPN > SSL VPN > SSL VPN Client**. The SSL VPN Client screen displays (see *Figure 127* on page 206).
2. In the Add Routes for VPN Tunnel Clients section of the screen, specify information in the following fields:
   - **Destination Network**. The destination network IP address of a local network or subnet. For example, enter 192.168.1.60.
   - **Subnet Mask**. The address of the appropriate subnet mask.
3. Click the **Add** table button. The new client route is added to the Configured Client Routes table.

Note: If VPN tunnel clients are already connected, restart the VPN firewall. Restarting forces clients to reconnect and receive new addresses and routes.

➤ **To change the specifications of an existing route and to delete an old route:**

1. Add a new route to the Configured Client Routes table.

2. In the Configured Client Routes table, to the right of the route that is out-of-date, click the **Delete** table button.

If an existing route is no longer needed for any reason, you can delete it.

Use Network Resource Objects to Simplify Policies

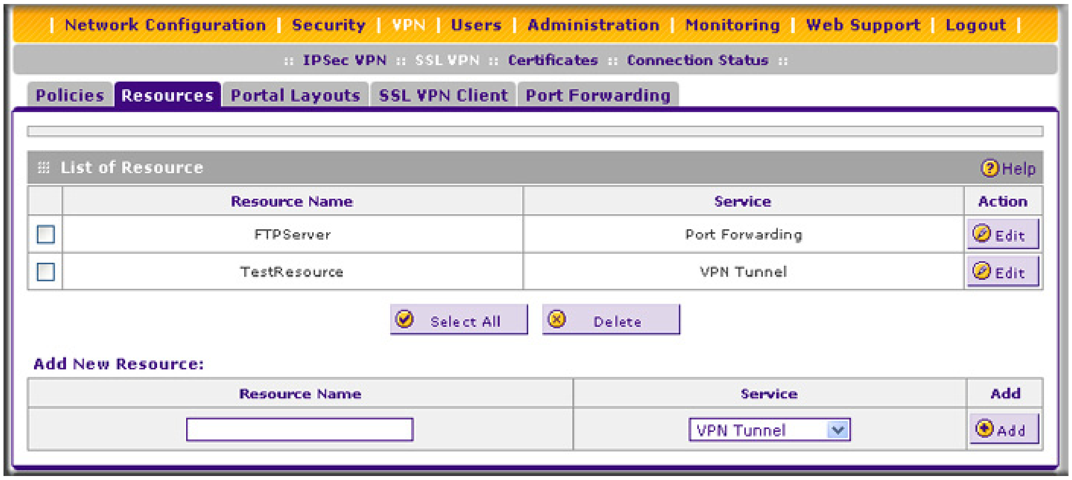
Network resources are groups of IP addresses, IP address ranges, and services. By defining resource objects, you can more quickly create and configure network policies. You do not need to redefine the same set of IP addresses or address ranges when you configure the same access policies for multiple users.

Defining network resources is optional; smaller organizations can choose to create access policies using individual IP addresses or IP networks rather than predefined network resources. But for most organizations, NETGEAR recommends that you use network resources. If your server or network configuration changes, you can perform an update quickly by using network resources instead of individually updating all of the user and group policies.

Add New Network Resources

➤ **To define a network resource:**

1. Select **VPN > SSL VPN > Resources**. The Resources screen displays. (The following figure shows some resources in the List of Resources table as an example.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: Certificates :: Connection Status ::
Policies
Resources
Portal Layouts
SSL VPN Client
Port Forwarding
Help
Select All
Delete
Add

List of Resource

	Resource Name	Service	Action
□	FTPServer	Port Forwarding	Edit
□	TestResource	VPN Tunnel	Edit

Add New Resource:

Resource Name	Service	Add
	VPN Tunnel	Add

Figure 128.

2. In the Add New Resource section of the screen, specify information in the following fields:
   - **Resource Name**. A descriptive name of the resource for identification and management purposes.
   - **Service**. From the Service drop-down list, select the type of service to which the resource applies:
     - **VPN Tunnel**. The resource applies only to a VPN tunnel.

- **Port Forwarding**. The resource applies only to a port forwarding.
- **All**. The resource applies both to a VPN tunnel and to port forwarding.

3. Click the **Add** table button. The new resource is added to the List of Resources table.

➤ **To delete one or more network resources:**

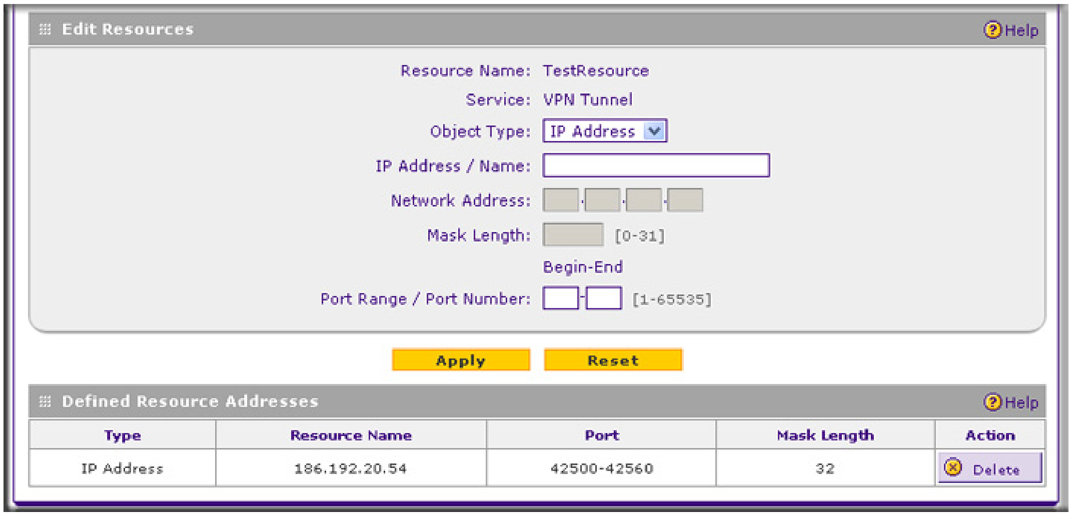
1. Select the check box to the left of the network resource that you want to delete, or click the **Select All** table button to select all VPN policies.
2. Click the **Delete** table button.

Edit Network Resources to Specify Addresses

After you have defined a resource on the Resources screen, you can assign an IP or network address and a port or port range to the resource.

➤ **To edit a resource:**

1. Select **VPN > SSL VPN > Resources**. The Resources screen displays (see the previous figure, which shows some examples).
2. In the List of Resources table, to the right of the new resource in the Action column, click the **Edit** table button. A new screen displays. (The following figure shows an example.)



Resource Name: TestResource
Service: VPN Tunnel
Object Type: IP Address
IP Address / Name:
Network Address: . . .
Mask Length: [0-31]
Begin-End
Port Range / Port Number: - [1-65535]

Type	Resource Name	Port	Mask Length	Action
IP Address	186.192.20.54	42500-42560	32	Delete

Figure 129.

3. Complete the settings as explained the following table:

Table 53. Edit Resources screen settings

Setting	Description
Resource Name	The unique identifier for the resource. For information only. (You cannot edit the resource name after you have created it on the Resources screen.)
Service	The SSL service that is assigned to the resource. For information only. (You cannot edit the service after you have assigned it to the resource on the Resources screen.)

Table 53. Edit Resources screen settings (continued)

Setting	Description	
Object Type	From the drop-down list, select one of the following options: • **IP Address**. The object is an IP address. You need to enter the IP address or the FQDN in the IP Address / Name field. • **IP Network**. The object is an IP network. You need to enter the network IP address in the Network Address field and the network mask length in the Mask Length field.	
	IP Address / Name	Applicable only when you select IP Address as the object type. Enter the IP address or FQDN for the location that is permitted to use this resource.
	Network Address	Applicable only when you select IP Network as the object type. Enter the network IP address for the locations that are permitted to use this resource.
	Mask Length	Applicable only when you select IP Network as the object type. As an option, enter the network mask (0–31) for the locations that are permitted to use this resource.
Port Range / Port Number	A port or a range of ports (0–65535) to apply the policy to; the policy is applied to all TCP and UDP traffic that passes on those ports. Leave the fields blank to apply the policy to all traffic.	

4. Click **Apply** to save your settings. The new configuration is added to the Defined Resource Addresses table.

To delete a configuration from the Defined Resource Addresses table, click the **Delete** table button to the right of the configuration that you want to delete.

Configure User, Group, and Global Policies

You can define and apply user, group, and global policies to predefined network resource objects, IP addresses, address ranges, or all IP addresses, and to different SSL VPN services. A specific hierarchy is invoked over which policies take precedence. The VPN firewall policy hierarchy is defined as follows:

1. User policies take precedence over all group policies.
2. Group policies take precedence over all global policies.
3. If two or more user, group, or global policies are configured, the *most specific* policy takes precedence.

For example, a policy that is configured for a single IP address takes precedence over a policy that is configured for a range of addresses. And a policy that applies to a range of IP addresses takes precedence over a policy that is applied to all IP addresses. If two or more IP address ranges are configured, then the smallest address range takes precedence. Host names are treated the same as individual IP addresses.

Network resources are prioritized just like other address ranges. However, the prioritization is based on the individual address or address range, not the entire network resource.

For example, assume the following global policy configuration:

- Policy 1. A Deny rule has been configured to block all services to the IP address range 10.0.0.0 – 10.0.0.255.
- Policy 2. A Deny rule has been configured to block FTP access to 10.0.1.2–10.0.1.10.
- Policy 3. A Permit rule has been configured to allow FTP access to the predefined network resource with the name FTP Servers. The FTP Servers network resource includes the following addresses: 10.0.0.5–10.0.0.20 and the FQDN ftp.*company*.com, which resolves to 10.0.1.3.

Assuming that no conflicting user or group policies have been configured, if a user would attempt to access:

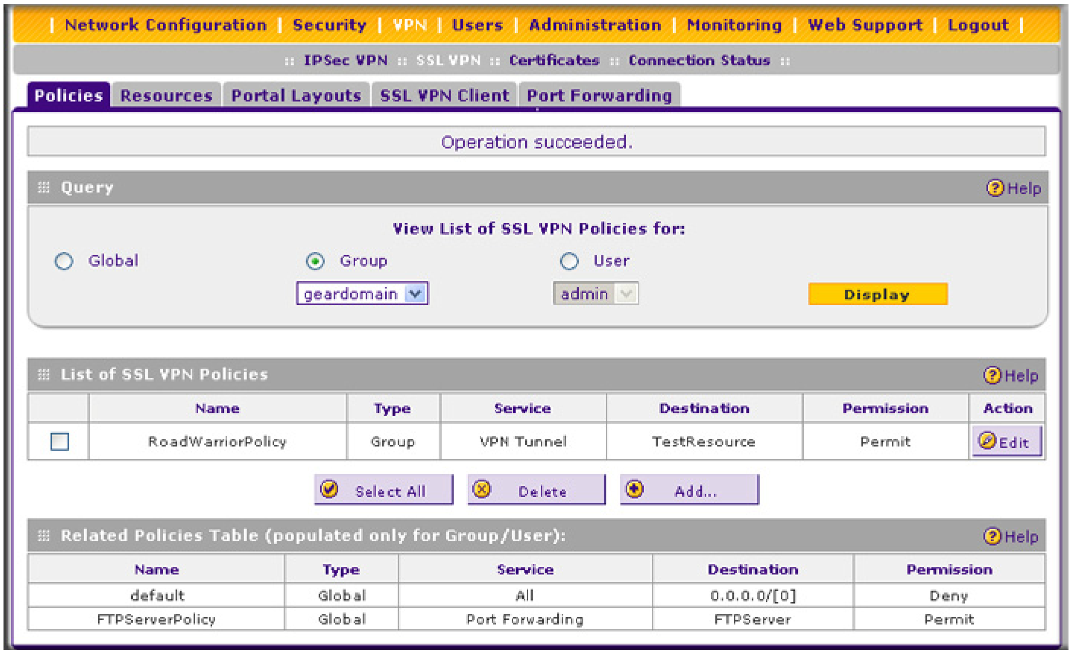
- an FTP server at 10.0.0.1, the user would be blocked by Policy 1.
- an FTP server at 10.0.1.5, the user would be blocked by Policy 2.
- an FTP server at 10.0.0.10, the user would be granted access by Policy 3. The IP address range 10.0.0.5–10.0.0.20 is more specific than the IP address range that is defined in Policy 1.
- an FTP server at ftp.*company*.com, the user would be granted access by Policy 3. A single host name is more specific than the IP address range that is configured in Policy 2

Note: The user would not be able to access ftp.*company*.com using its IP address 10.0.1.3. The VPN firewall’s policy engine does not perform reverse DNS lookups.

View Policies

➤ **To view the existing policies, follow these steps:**

1. Select **VPN > SSL VPN**. The SSL VPN submenu tabs display, with the Policies screen in view. (The following figure shows some examples.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: Certificates :: Connection Status ::
Policies
Resources
Portal Layouts
SSL VPN Client
Port Forwarding
Help
Display
Select All
Delete
Add...
Edit

Operation succeeded.

Query

View List of SSL VPN Policies for:

○ Global ● Group ○ User

Group: geardomain; User: admin

List of SSL VPN Policies

	Name	Type	Service	Destination	Permission	Action
□	RoadWarriorPolicy	Group	VPN Tunnel	TestResource	Permit	Edit

Related Policies Table (populated only for Group/User):

Name	Type	Service	Destination	Permission
default	Global	All	0.0.0.0/[0]	Deny
FTPServerPolicy	Global	Port Forwarding	FTPServer	Permit

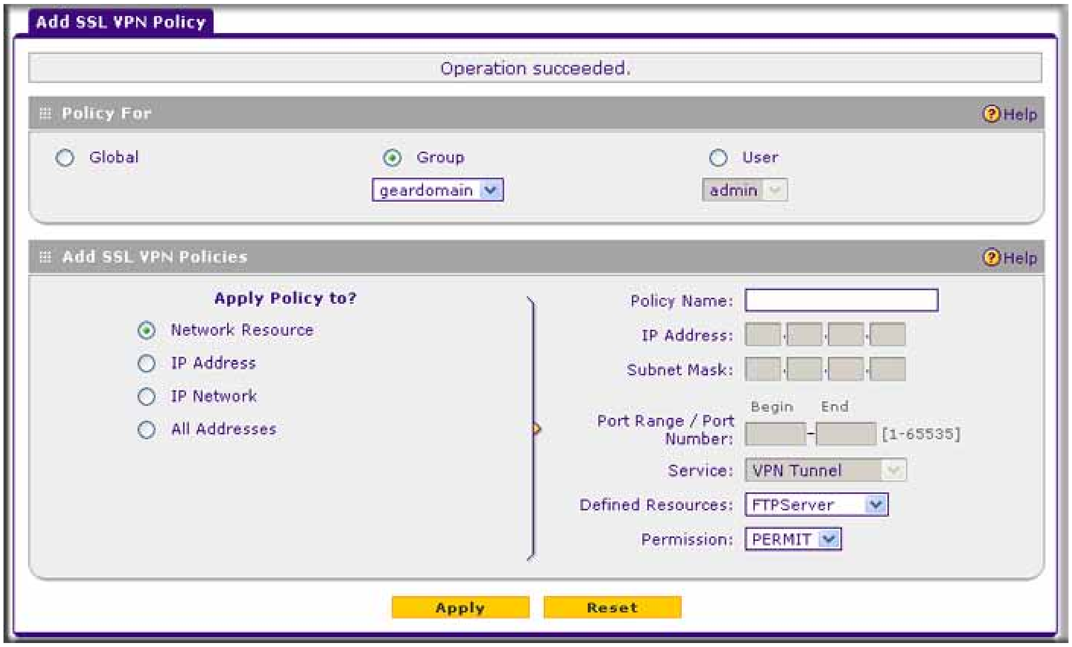
Figure 130.

2. Make your selection from the following Query options:
   - Click **Global** to view all global policies.
   - Click **Group** to view group policies, and choose the relevant group's name from the drop-down list.
   - Click **User** to view user policies, and choose the relevant user's name from the drop-down list.
3. Click the **Display** action button. The List of SSL VPN Policies table displays the list for your selected Query option.

Add a Policy

➢ To add an SSL VPN policy:

1. Select **VPN > SSL VPN**. The SSL VPN submenu tabs display, with the Policies screen in view (see the previous figure, which shows some examples).
2. Under the List of SSL VPN Policies table, click the **Add** table button. The Add Policy screen displays:



Add SSL VPN Policy

Operation succeeded.

Policy For

○ Global ● Group: geardomain ○ User: admin

Add SSL VPN Policies

Apply Policy to?

● Network Resource
○ IP Address
○ IP Network
○ All Addresses

Policy Name:
IP Address:
Subnet Mask:
Port Range / Port Number: Begin – End [1-65535]
Service: VPN Tunnel
Defined Resources: FTPServer
Permission: PERMIT

Figure 131.

3. Complete the settings as explained the following table:

Table 54. Add SSL VPN Policy screen settings

Setting	Description
Policy For	
Select one of the following radio buttons to specify the type of SSL VPN policy: • **Global**. The new policy is global and excludes all groups and users. • **Group**. The new policy is limited to a single group. From the drop-down list, select a group name. • **User**. The new policy is limited to a single user. From the drop-down list, select a user name. **Note:** For information about how to create groups, see *Configure Groups for VPN Policies* on page 224. For information about how to create user accounts, see *Configure User Accounts* on page 227.	

Table 54. Add SSL VPN Policy screen settings (continued)

Setting	Description		
Add SSL VPN Policies			
Apply Policy For	Select one of the following radio buttons to specify how the policy is applied: • **Network Resource**. The policy is applied to a network resource that you have defined on the Resources screen (see *Use Network Resource Objects to Simplify Policies* on page 208). The screen adjusts to display the fields that are shown in the Network Resource rows. • **IP Address**. The policy is applied to a single IP address. The screen adjusts to display the fields that are shown in the IP Address rows of this table. • **IP Network**. The policy is applied to a network address. The screen adjusts to display the fields that are shown in the IP Network rows of this table. • **All Addresses**. The policy is applied to all addresses. The screen adjusts to display the fields that are shown in the All Addresses rows of this table.		
	Network Resource	Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.
		Defined Resources	From the drop-down list, select a network resource that you have defined on the Resources screen (see *Use Network Resource Objects to Simplify Policies* on page 208).
		Permission	From the drop-down list, select whether the policy permits (**PERMIT**) or denies (**DENY**) access.
	IP Address	Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.
		IP Address	The IP address to which the SSL VPN policy is applied.
		Port Range / Port Number	A port (enter in the Begin field) or a range of ports (enter in the Begin and End fields) to which the SSL VPN policy is applied. Ports can be 0 through 65535. The policy is applied to all TCP and UDP traffic that passes on those ports. Leave the fields blank to apply the policy to all traffic.
		Service	From the drop-down list, select the service to which the SSL VPN policy is applied: • **VPN Tunnel**. The policy is applied only to a VPN tunnel. • **Port Forwarding**. The policy is applied only to port forwarding. • **All**. The policy is applied both to a VPN tunnel and to port forwarding.
		Permission	From the drop-down list, select whether the policy permits (**PERMIT**) or denies (**DENY**) access.

Table 54. Add SSL VPN Policy screen settings (continued)

Setting	Description		
Apply Policy For (continued)	IP Network	Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.
		IP Address	The network IP address to which the SSL VPN policy is applied.
		Subnet Mask	The network subnet mask to which the SSL VPN policy is applied.
		Port Range / Port Number	A port (enter in the Begin field) or a range of ports (enter in the Begin and End fields) to which the SSL VPN policy is applied. Ports can be 0 through 65535. The policy is applied to all TCP and UDP traffic that passes on those ports. Leave the fields blank to apply the policy to all traffic.
		Service	From the drop-down list, select the service to which the SSL VPN policy is applied: • **VPN Tunnel**. The policy is applied only to a VPN tunnel. • **Port Forwarding**. The policy is applied only to port forwarding. • **All**. The policy is applied both to a VPN tunnel and to port forwarding.
		Permission	From the drop-down list, select whether the policy permits (**PERMIT**) or denies (**DENY**) access.
	All Addresses	Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.
		Port Range / Port Number	A port (enter in the Begin field) or a range of ports (enter in the Begin and End fields) to which the SSL VPN policy is applied. Ports can be 0 through 65535. The policy is applied to all TCP and UDP traffic that passes on those ports. Leave the fields blank to apply the policy to all traffic.
		Service	From the drop-down list, select the service to which the SSL VPN policy is applied: • **VPN Tunnel**. The policy is applied only to a VPN tunnel. • **Port Forwarding**. The policy is applied only to port forwarding. • **All**. The policy is applied both to a VPN tunnel and to port forwarding.
		Permission	From the drop-down list, select whether the policy permits (**PERMIT**) or denies (**DENY**) access.

4. Click **Apply** to save your settings. The policy is added to the List of SSL VPN Policies table on the Policies screen. The new policy goes into effect immediately.

Note: If you have configured SSL VPN user policies, ensure that HTTPS remote management is enabled (see *Configure Remote Management Access* on page 250). If HTTPS remote management is not enabled, all SSL VPN user connections are disabled.

➢ **To edit an SSL VPN policy:**

1. On the Policies screen (see *Figure 130* on page 212), click the **Edit** button in the Action column for the SSL VPN policy that you want to modify. The Edit SSL VPN Policy screen displays. This screen is identical to the Add SSL VPN Policy screen (see previous screen).
2. Modify the settings as explained in the previous table.
3. Click **Apply** to save your settings.

➢ **To delete one or more SSL VPN policies:**

1. On the Policies screen (see *Figure 130* on page 212), select the check box to the left of the SSL VPN policy that you want to delete, or click the **Select All** table button to select all policies.
2. Click the **Delete** table button.

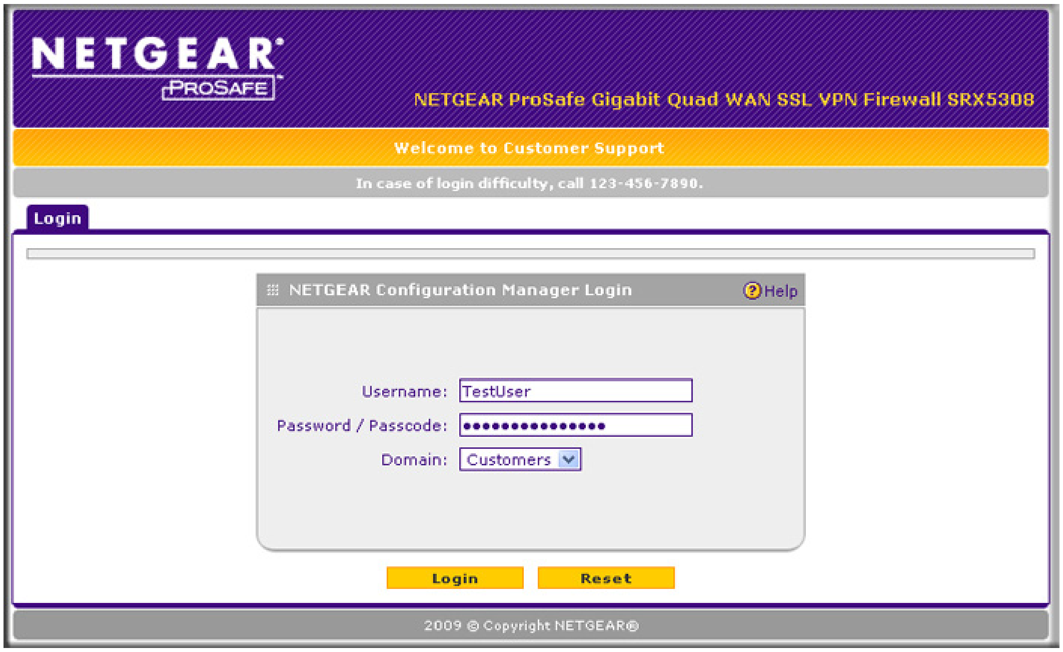
Access the SSL Portal Login Screen

All screens that you can access from the SSL VPN menu of the web management interface display a user portal link at the right upper corner, above the menu bars (User Portal).

When you click the user portal link, the SSL VPN default portal opens (see *Figure 133* on page 217). This user portal is not the same as the new SSL portal login screen that you defined in *Create the Portal Layout* on page 198.

➢ **To open the new SSL portal login screen:**

1. Select **VPN > SSL VPN > Portal Layouts**. The Portal Layout screen displays (see *Figure 124* on page 199).
2. In the Portal URL column of the List of Layouts table, click a URL. The new SSL portal login screen displays. (The following figure displays the previously created CustomerSupport portal layout as an example).



NETGEAR ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

Welcome to Customer Support

In case of login difficulty, call 123-456-7890.

NETGEAR Configuration Manager Login

Username: TestUser

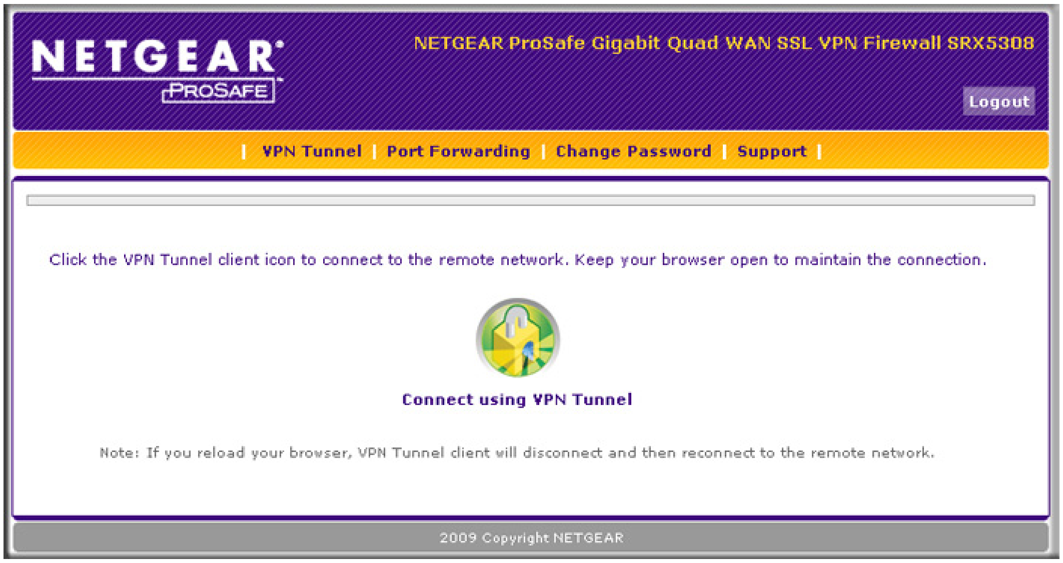
Password / Passcode: •••••••••••••••

Domain: Customers

2009 © Copyright NETGEAR®

Figure 132.

3. Enter a user name and password that are associated with the SSL portal and the domain (see *Configure VPN Authentication Domains, Groups, and Users* on page 219).
4. Click **Login**. The default User Portal screen displays:


NETGEAR
PROSAFE
Logout
| VPN Tunnel | Port Forwarding | Change Password | Support |
Connect using VPN Tunnel

NETGEAR ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308

Click the VPN Tunnel client icon to connect to the remote network. Keep your browser open to maintain the connection.

Note: If you reload your browser, VPN Tunnel client will disconnect and then reconnect to the remote network.

2009 Copyright NETGEAR

Figure 133.

The default User Portal screen displays a simple menu that provides the SSL user with the following menu selections:

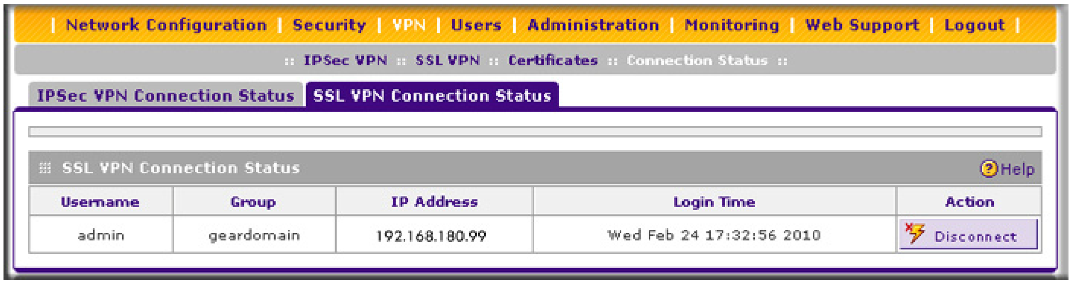
- **VPN Tunnel**. Provides full network connectivity.
- **Port Forwarding**. Provides access to the network services that you defined in *Configure Applications for Port Forwarding* on page 202.

- **Change Password**. Allows the user to change their password.
- **Support**. Provides access to the NETGEAR website.

View the SSL VPN Connection Status and SSL VPN Logs

➤ **To review the status of current SSL VPN tunnels:**

Select **VPN > Connection Status > SSL VPN Connection Status**. The SSL VPN Connection Status screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: Certificates :: Connection Status ::
IPSec VPN Connection Status
SSL VPN Connection Status
?Help

SSL VPN Connection Status

Username	Group	IP Address	Login Time	Action
admin	geardomain	192.168.180.99	Wed Feb 24 17:32:56 2010	Disconnect

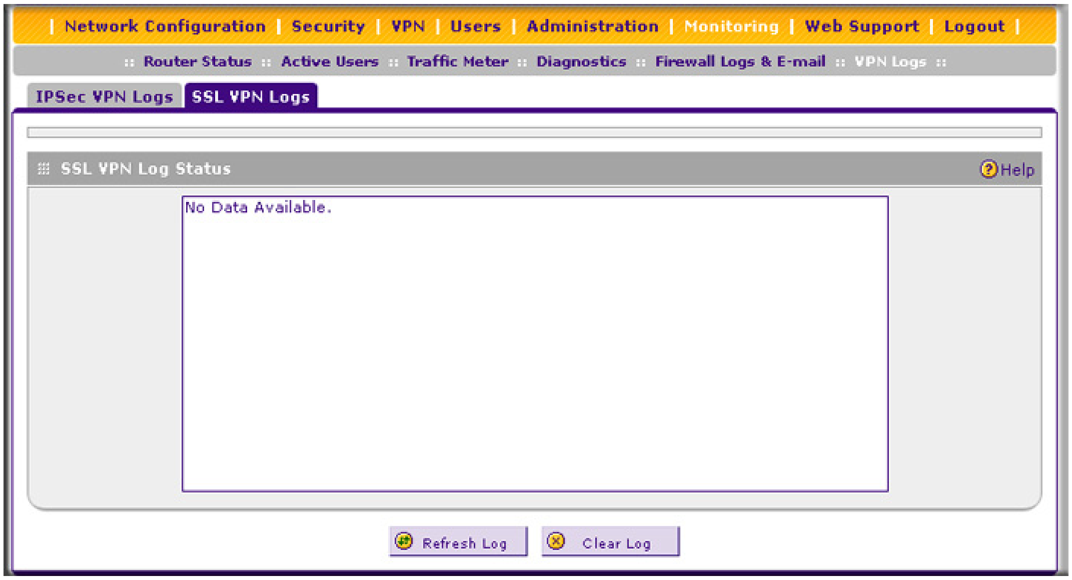
Figure 134.

The active user’s user name, group, and IP address are listed in the table with a timestamp indicating the time and date that the user connected.

To disconnect an active user, click the **Disconnect** table button to the right of the user’s table entry.

➤ **To view the SSL VPN Logs:**

Select Monitoring > **VPN Logs** > **SSL VPN Logs**. The SSL VPN Logs screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
IPSec VPN Logs
SSL VPN Logs
SSL VPN Log Status
?Help
Refresh Log
Clear Log

```
No Data Available.
```

Figure 135.

Managing Users, Authentication, and Certificates 7

This chapter describes how to manage users, authentication, and security certificates for IPSec VPN and SSL VPN. This chapter contains the following sections:

- *Configure VPN Authentication Domains, Groups, and Users*
- *Manage Digital Certificates*

Configure VPN Authentication Domains, Groups, and Users

Users are assigned to a group, and a group is assigned to a domain. Therefore, you should first create any domains, then groups, then user accounts.

You need to create name and password accounts for all users who should be able connect to the VPN firewall. This includes administrators and SSL VPN clients. Accounts for IPSec VPN clients are required only if you have enabled Extended Authentication (XAUTH) in your IPSec VPN configuration.

Users connecting to the VPN firewall need to be authenticated before being allowed to access the VPN firewall or the VPN-protected network. The login window that is presented to the user requires three items: a user name, a password, and a domain selection. The domain determines the authentication method that is used and, for SSL connections, the portal layout that is presented.

Note: IPSec VPN users always belong to the default domain (geardomain) and are not assigned to groups.

Except in the case of IPSec VPN users, when you create a user account, you need to specify a group. When you create a group, you need to specify a domain.

Configure Domains

The domain determines the authentication method to be used for associated users. For SSL connections, the domain also determines the portal layout that is presented, which in turn determines the network resources to which the associated users have access. The default domain of the VPN firewall is named geardomain. You cannot delete the default domain.

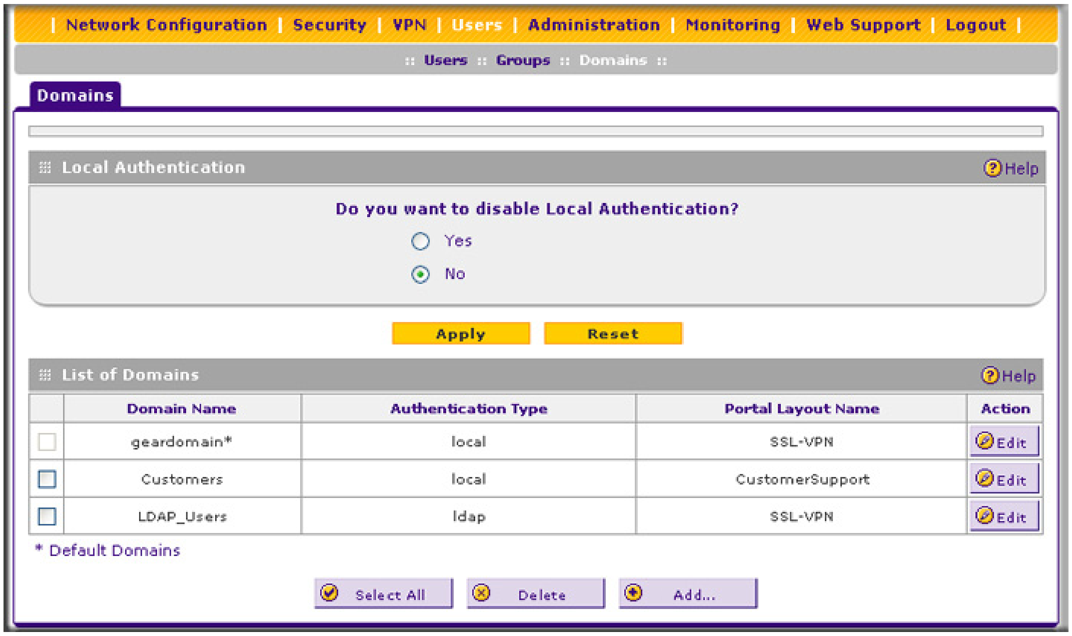
The following table summarizes the authentication protocols and methods that the VPN firewall supports:

Table 55. Authentication protocols and methods

Authentication protocol or method	Description
PAP	Password Authentication Protocol (PAP) is a simple protocol in which the client sends a password in clear text.
CHAP	Challenge Handshake Authentication Protocol (CHAP) executes a three-way handshake in which the client and server trade challenge messages, each responding with a hash of the other's challenge message that is calculated using a shared secret value.
RADIUS	A network-validated PAP or CHAP password-based authentication method that functions with Remote Authentication Dial In User Service (RADIUS).
MIAS	A network-validated PAP or CHAP password-based authentication method that functions with Microsoft Internet Authentication Service (MIAS), which is a component of Microsoft Windows 2003 Server.
WiKID	WiKID Systems is a PAP or CHAP key-based two-factor authentication method that functions with public key cryptography. The client sends an encrypted PIN to the WiKID server and receives a one-time pass code with a short expiration period. The client logs in with the passcode. See *Appendix D, Two-Factor Authentication* for more on WiKID authentication.
NT Domain	A network-validated domain-based authentication method that functions with a Microsoft Windows NT Domain authentication server. This authentication method has been superseded by Microsoft Active Directory authentication but is supported to authenticate legacy Windows clients.
Active Directory	A network-validated domain-based authentication method that functions with a Microsoft Active Directory authentication server. Microsoft Active Directory authentication servers support a group and user structure. Because the Active Directory supports a multilevel hierarchy (for example, groups or organizational units), this information can be queried to provide specific group policies or bookmarks based on Active Directory attributes. **Note:** A Microsoft Active Directory database uses an LDAP organization schema.
LDAP	A network-validated domain-based authentication method that functions with a Lightweight Directory Access Protocol (LDAP) authentication server. LDAP is a standard for querying and updating a directory. Because LDAP supports a multilevel hierarchy (for example, groups or organizational units), this information can be queried to provide specific group policies or bookmarks based on LDAP attributes.

➤ **To create a domain:**

1. Select **Users > Domains**. The Domains screen displays. The following figure shows the VPN firewall's default domain—geardomain—and, as an example, several other domains in the List of Domains table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Users :: Groups :: Domains ::
Domains
Local Authentication
Help
Apply
Reset
List of Domains
Help
Select All
Delete
Add...

Do you want to disable Local Authentication?

○ Yes
● No

	Domain Name	Authentication Type	Portal Layout Name	Action
□	geardomain*	local	SSL-VPN	Edit
□	Customers	local	CustomerSupport	Edit
□	LDAP_Users	ldap	SSL-VPN	Edit

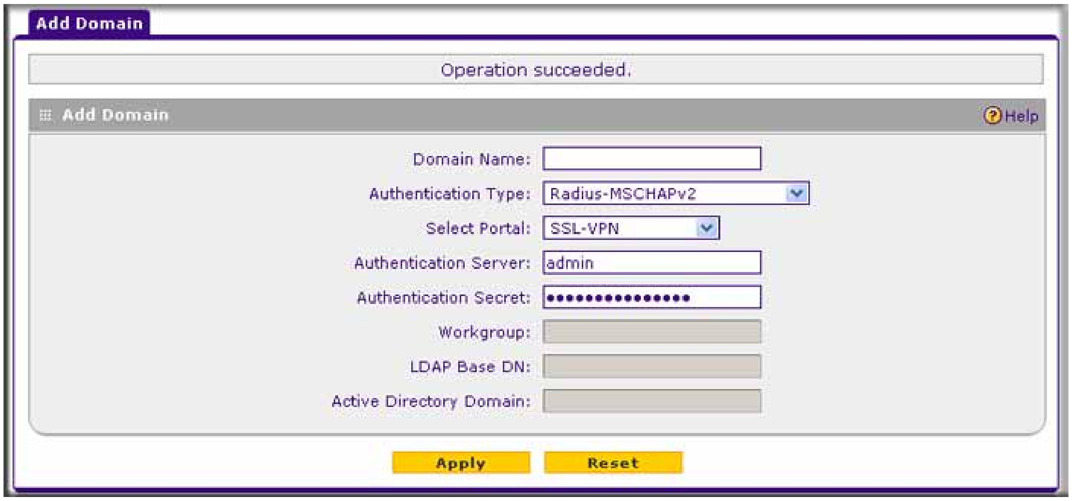
* Default Domains

Figure 136.

The List of Domains table displays the domains with the following fields:

- **Check box**. Allows you to select the domain in the table.
- **Domain Name**. The name of the domain. The default domain name (geardomain) is appended by an asterisk.
- **Authentication Type**. The authentication method that is assigned to the domain.
- **Portal Layout Name**. The SSL portal layout that is assigned to the domain.
- **Action**. The Edit table button that provides access to the Edit Domain screen.

2. Under the List of Domains table, click the **Add** table button. The Add Domain screen displays:



Operation succeeded.

Domain Name:	
Authentication Type:	Radius-MSCHAPv2
Select Portal:	SSL-VPN
Authentication Server:	admin
Authentication Secret:	•••••••••••••••
Workgroup:	
LDAP Base DN:	
Active Directory Domain:	

Figure 137.

3. Enter the settings as explained in the following table:

Table 56. Add Domain screen settings

Setting	Description
Domain Name	A descriptive (alphanumeric) name of the domain for identification and management purposes.
Authentication Type **Note:** If you select any type of RADIUS authentication, make sure that one or more RADIUS servers are configured (see *RADIUS Client Configuration* on page 174).	From the drop-down list, select the authentication method that the VPN firewall applies to the domain. The screen adjusts to display the fields that require configuration. • **Local User Database (default)**. Users are authenticated locally on the VPN firewall. This is the default setting. You do not need to complete any other fields on this screen. • **Radius-PAP**. RADIUS Password Authentication Protocol (PAP). Complete the Authentication Server and Authentication Secret fields. • **Radius-CHAP**. RADIUS Challenge Handshake Authentication Protocol (CHAP). Complete the Authentication Server and Authentication Secret fields. • **Radius-MSCHAP**. RADIUS Microsoft CHAP. Complete the Authentication Server and Authentication Secret fields. • **Radius-MSCHAPv2**. RADIUS Microsoft CHAP version 2. Complete the Authentication Server and Authentication Secret fields. • **WIKID-PAP**. WiKID Systems PAP. Complete the Authentication Server and Authentication Secret fields. • **WIKID-CHAP**. WiKID Systems CHAP. Complete the Authentication Server and Authentication Secret fields. • **MIAS-PAP**. Microsoft Internet Authentication Service (MIAS) PAP. Complete the Authentication Server and Authentication Secret fields. • **MIAS-CHAP**. Microsoft Internet Authentication Service (MIAS) CHAP. Complete the Authentication Server and Authentication Secret fields. • **NT Domain**. Microsoft Windows NT Domain. Complete the Authentication Server and Workgroup fields. • **Active Directory**. Microsoft Active Directory. Complete the Authentication Server and Active Directory Domain fields. • **LDAP**. Lightweight Directory Access Protocol (LDAP). Complete the Authentication Server and LDAP Base DN fields.
Select Portal	The drop-down list shows the SSL portals that are listed on the Portal Layout screen. From the drop-down list, select the SSL portal with which the domain is associated. For information about how to configure SSL portals, see *Create the Portal Layout* on page 198.
Authentication Server	The server IP address or server name of the authentication server for any type of authentication other than authentication through the local user database.
Authentication Secret	The authentication secret or password that is required to access the authentication server for RADIUS, WiKID, or MIAS authentication.
Workgroup	The workgroup that is required for Microsoft NT Domain authentication.
LDAP Base DN	The LDAP base distinguished name (DN) that is required for LDAP authentication.
Active Directory Domain	The active directory domain name that is required for Microsoft Active Directory authentication.

4. Click **Apply** to save your settings. The domain is added to the List of Domains table.
5. If you use local authentication, make sure that it is not disabled: Select the **No** radio button in the Local Authentication section of the Domain screen (see *Figure 136* on page 221).

Note: A combination of local and external authentication is supported.

WARNING!

If you disable local authentication, make sure that there is at least one external administrative user; otherwise, access to the VPN firewall is blocked.

6. If you change local authentication, click **Apply** in the Domain screen to save your settings.

➢ **To delete one or more domains:**

1. In the List of Domains table, select the check box to the left of the domain that you want to delete, or click the **Select All** table button to select all domains. You cannot delete a default domain.
2. Click the **Delete** table button.

Edit Domains

➢ **To edit a domain:**

1. Select **Users > Domains**. The Domains screen displays (see *Figure 136* on page 221).
2. In the Action column of the List of Domains table, click the **Edit** table button for the domain that you want to edit. The Edit Domains screen displays. This screen is very similar to the Add Domains screen (see the previous figure).
3. Modify the settings as explained in the previous table. (You cannot modify the Domain Name and Authentication Type fields.)
4. Click **Apply** to save your changes. The modified domain is displayed in the List of Domains table.

Note: You cannot edit the geardomain default domain.

Configure Groups for VPN Policies

The use of groups simplifies the configuration of VPN policies when different sets of users have different restrictions and access controls. Like the default domain of the VPN firewall, the default group is also named geardomain. The default group geardomain is assigned to the default domain geardomain. You cannot delete the default domain geardomain, nor its associated default group geardomain.

IMPORTANT:

When you create a new domain on the Domains screen (see the previous section), a default group with the same name as the new domain is created automatically. The name of a default group is appended by an asterisk, and you cannot delete a default group. However, when you delete the domain with which it is associated, the default group is deleted automatically.

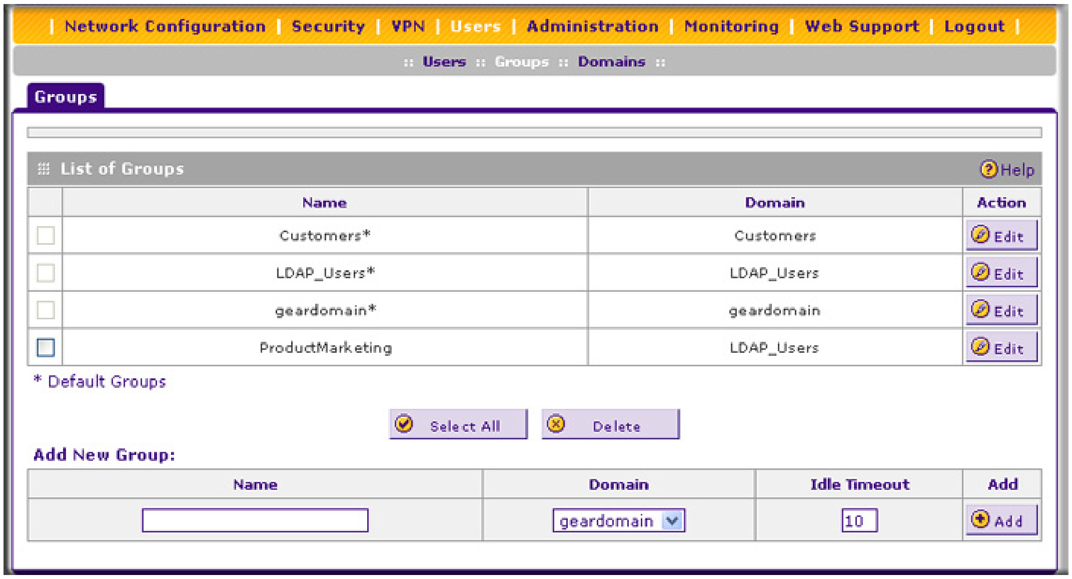
Note: IPSec VPN users always belong to the default domain (geardomain) and are not assigned to groups.

Note: Groups that are defined on the User screen are used for setting SSL VPN policies. These groups should not be confused with LAN groups that are defined on the LAN Groups screen and that are used to simplify firewall policies. For information about LAN groups, see *Manage Groups and Hosts (LAN Groups)* on page 67.

Create and Delete Groups

➢ **To create a VPN group:**

1. Select **Users > Groups**. The Groups screen displays. The following figure shows the VPN firewall's default group—geardomain—and, as an example, several other groups in the List of Groups table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Users :: Groups :: Domains ::
Groups
List of Groups
Help
Select All
Delete
Add New Group:
Add

List of Groups

	Name	Domain	Action
□	Customers*	Customers	Edit
□	LDAP_Users*	LDAP_Users	Edit
□	geardomain*	geardomain	Edit
□	ProductMarketing	LDAP_Users	Edit

* Default Groups

Add New Group:

Name	Domain	Idle Timeout	Add
	geardomain	10	Add

Figure 138.

The List of Groups table displays the VPN groups with the following fields:

- **Check box**. Allows you to select the group in the table.
- **Name**. The name of the group. If the group name is appended by an asterisk, the group was created by default when you created the domain with the identical name as the default group. You cannot delete a default group; you can only delete the domain with the identical name, which causes the default group to be deleted.
- **Domain**. The name of the domain to which the group is assigned.
- **Action**. The Edit table button that provides access to the Edit Group screen.

2. In the Add New Group section of the screen, enter the settings as explained in the following table:

Table 57. Group screen settings

Setting	Description
Name	A descriptive (alphanumeric) name of the group for identification and management purposes.
Domain	The drop-down list shows the domains that are listed on the Domain screen. From the drop-down list, select the domain with which the group is associated. For information about how to configure domains, see *Configure Domains* on page 219.
Idle Timeout	The period after which an idle user is automatically logged out of the VPN firewall's web management interface. The default idle time-out period is 10 minutes.

3. Click the **Add** table button. The new group is added to the List of Groups table.

➤ To delete one or more groups:

1. In the List of Groups table, select the check box to the left of the group that you want to delete, or click the **Select All** table button to select all groups. You cannot delete a

default group; you can only delete the domain with the identical name as the default group (see *Configure Domains* on page 219), which causes the default group to be deleted.

2. Click the **Delete** table button.

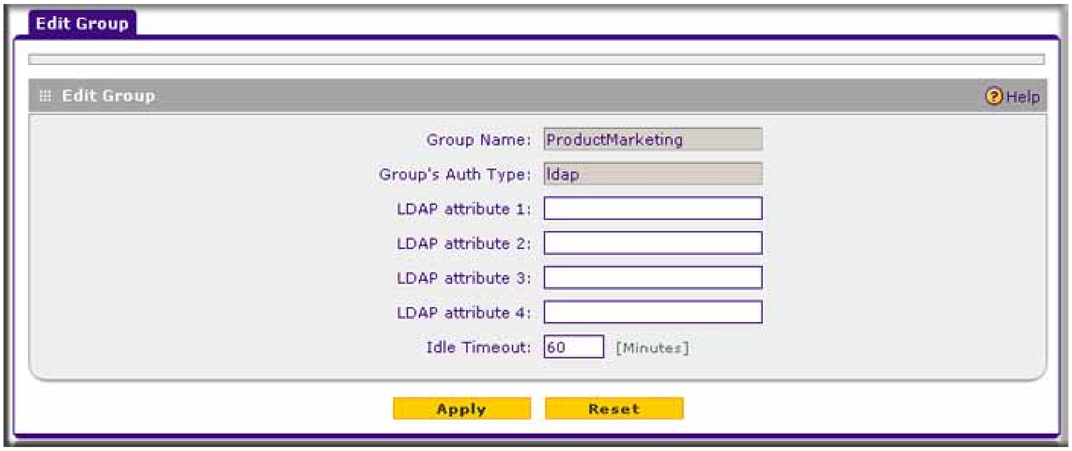
Note: You can delete only groups that you created on the Groups screen. Groups that were automatically created when you created a domain cannot be deleted on the Groups screen. See the Important note at the beginning of this section.

Edit Groups

➤ **To edit a VPN group:**

1. Select **Users > Groups**. The Groups screen displays (see the previous screen).
2. In the Action column of the List of Groups table, click the **Edit** table button for the group that you want to edit. The Edit Groups screen displays (see the following figure).

   With the exception of groups that are associated with domains that use the LDAP authentication method, you can modify only the idle time-out settings on the Edit Groups screen.



Group Name: ProductMarketing

Group's Auth Type: ldap

LDAP attribute 1:

LDAP attribute 2:

LDAP attribute 3:

LDAP attribute 4:

Idle Timeout: 60 [Minutes]

Figure 139.

3. Modify the idle time-out period in minutes in the Idle Timeout field. For a group that is associated with a domain that uses the LDAP authentication method, configure the LDAP attributes (in fields 1 through 4) as needed.
4. Click **Apply** to save your changes. The modified group is displayed in the List of Groups table.

Configure User Accounts

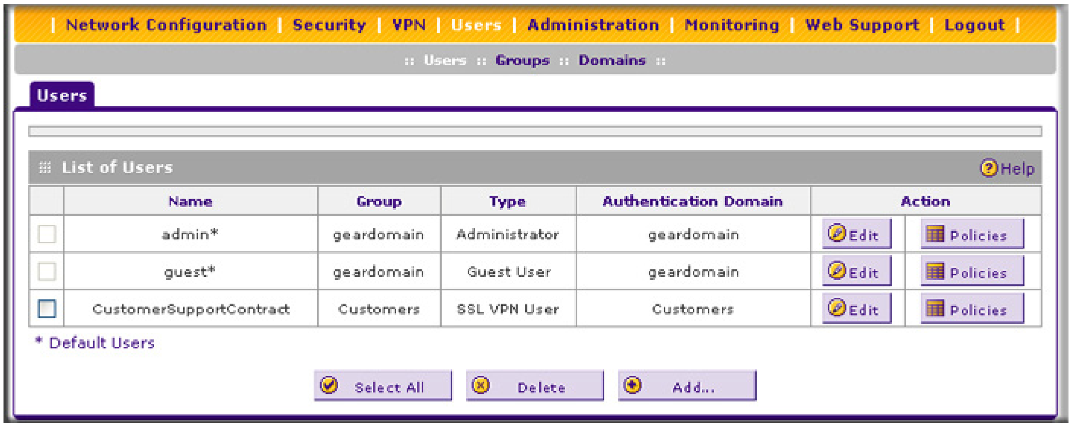
When you create a user account, you need to assign the user to a user group. When you create a group, you need to assign the group to a domain that specifies the authentication method. Therefore, you should first create any domains, then groups, and then user accounts.

You can create different types of user accounts by applying predefined user types:

- **Administrator**. A user who has full access and the capacity to change the VPN firewall configuration (that is, read/write access).
- **SSL VPN User**. A user who can only log in to the SSL VPN portal.
- **IPSEC VPN User**. A user who can only make an IPSec VPN connection via a NETGEAR ProSafe VPN Client, and only when the XAUTH feature is enabled (see *Configure Extended Authentication (XAUTH)* on page 172).
- **Guest user**. A user who can only view the VPN firewall configuration (that is, read-only access).

➢ **To create an individual user account:**

1. Select **Users > Users**. The Users screen displays. The following figure shows the VPN firewall's default users—admin and guest—and, as an example, another user in the List of Users table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Users :: Groups :: Domains ::
Users
List of Users
Help

	Name	Group	Type	Authentication Domain	Action	
□	admin*	geardomain	Administrator	geardomain	Edit	Policies
□	guest*	geardomain	Guest User	geardomain	Edit	Policies
□	CustomerSupportContract	Customers	SSL VPN User	Customers	Edit	Policies

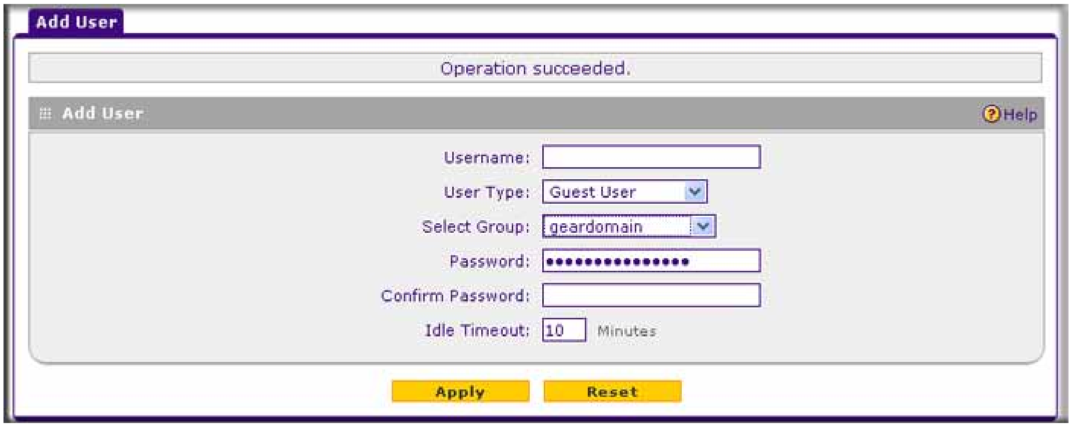
* Default Users

Figure 140.

The List of Users table displays the users with the following fields:

- **Check box**. Allows you to select the user in the table.
- **Name**. The name of the user. If the user name is appended by an asterisk, the user is a default user that came preconfigured with the VPN firewall and cannot be deleted.
- **Group**. The group to which the user is assigned.
- **Type**. The type of access credentials that are assigned to the user.
- **Authentication Domain**. The authentication domain to which the user is assigned.
- **Action**. The Edit table button that provides access to the Edit User screen; the Policies table button that provides access to the policy screens.

2. Click the **Add** table button. The Add User screen displays:



Add User

Operation succeeded.

Add User

Username:

User Type: Guest User

Select Group: geardomain

Password: ●●●●●●●●●●●●●●●

Confirm Password:

Idle Timeout: 10 Minutes

Figure 141.

3. Enter the settings as explained in the following table:

Table 58. Add User screen settings

Setting	Description
User Name	A descriptive (alphanumeric) name of the user for identification and management purposes.
User Type	From the drop-down list, select one of the predefined user types that determines the access credentials: • **Administrator**. User who has full access and the capacity to change the VPN firewall configuration (that is, read/write access). • **SSL VPN User**. User who can only log in to the SSL VPN portal. • **IPSEC VPN User**. User who can only make an IPSec VPN connection via a NETGEAR ProSafe VPN Client, and only when the XAUTH feature is enabled (see *Configure Extended Authentication (XAUTH)* on page 172). • **Guest User**. User who can only view the VPN firewall configuration (that is, read-only access).
Select Group	The drop-down list shows the groups that are listed on the Group screen. From the drop-down list, select the group to which the user is assigned. For information about how to configure groups, see *Configure Groups for VPN Policies* on page 224. **Note:** The user is automatically assigned to the domain that is associated with the selected group.
Password	The password that the user needs to enter to gain access to the VPN firewall. The password can contain alphanumeric, “—” or “_” characters.
Confirm Password	The password in this field needs to be identical to the one in the Password field.
Idle Timeout	The period after which an idle user is automatically logged out of the web management interface. The default idle time-out period is 10 minutes.

4. Click **Apply** to save your settings. The user is added to the List of Users table.

➢ **To delete one or more user accounts:**

1. In the List of Users table, select the check box to the left of the user account that you want to delete, or click the **Select All** table button to select all accounts. You cannot delete a default user account.
2. Click the **Delete** table button.

Note: You cannot delete the default admin or guest user.

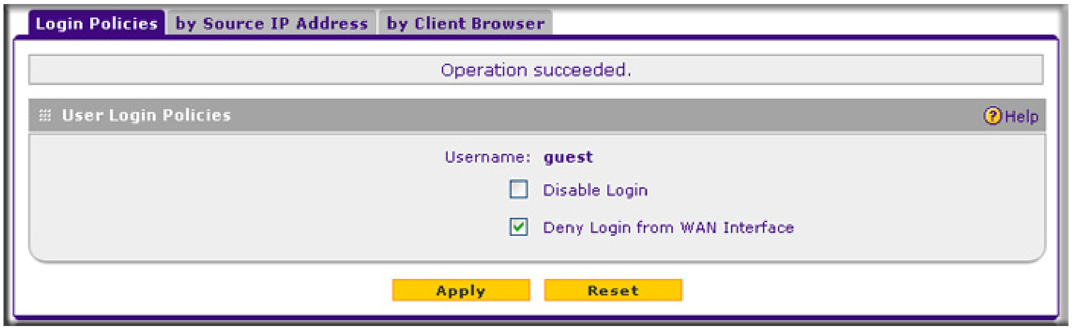
Set User Login Policies

You can restrict the ability of defined users to log in to the VPN firewall's web management interface. You can also require or prohibit logging in from certain IP addresses or from particular browsers.

Configure Login Policies

➢ **To configure user login policies:**

1. Select **Users > Users**. The Users screen displays (see *Figure 140* on page 227).
2. In the Action column of the List of Users table, click the **Policies** table button for the user for which you want to set login policies. The Policies submenu tabs display, with the Login Policies screen in view:



Operation succeeded.

User Login Policies

Username: guest

□ Disable Login

☑ Deny Login from WAN Interface

Figure 142.

3. In the User Login Policies section of the screen, make the following selections:
   - To prohibit this user from logging in to the VPN firewall, select the **Disable Login** check box.
   - To prohibit this user from logging in from the WAN interface, select the **Deny Login from WAN Interface** check box. In this case, the user can log in only from the LAN interface.

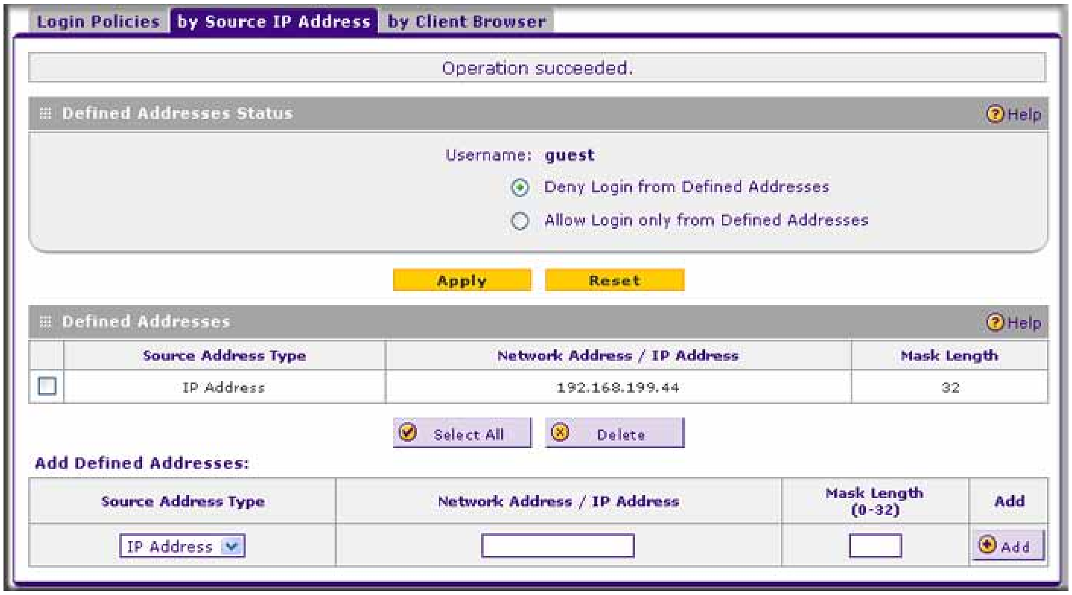
Note: For security reasons, the **Deny Login from WAN Interface** check box is selected by default for guests and administrators. The **Disable Login** check box is disabled (masked out) for administrators.

4. Click **Apply** to save your settings.

Configure Login Restrictions Based on IP Address

➢ **To restrict logging in based on IP address:**

1. Select **Users > Users**. The Users screen displays (see *Figure 140* on page 227).
2. In the Action column of the List of Users table, click the **Policies** table button for the user for which you want to set login policies. The Policies submenu tabs display, with the Login Policies screen in view.
3. Click the **by Source IP Address** submenu tab. The By Source IP Address screen displays. (The following figure shows an IP address in the Defined Addresses table as an example.)



Operation succeeded.

Defined Addresses Status

Username: guest

● Deny Login from Defined Addresses

○ Allow Login only from Defined Addresses

Defined Addresses

	Source Address Type	Network Address / IP Address	Mask Length
□	IP Address	192.168.199.44	32

Add Defined Addresses:

Source Address Type	Network Address / IP Address	Mask Length (0-32)	Add
IP Address			Add

Figure 143.

4. In the Defined Addresses Status section of the screen, select one of the following radio buttons:
   - **Deny Login from Defined Addresses**. Deny logging in from the IP addresses in the Defined Addresses table.
   - **Allow Login only from Defined Addresses**. Allow logging in from the IP addresses in the Defined Addresses table.
5. Click **Apply** to save your settings.

6. In the Add Defined Addresses section of the screen, add an address to the Defined Addresses table by entering the settings as explained in the following table:

Table 59. Defined addresses settings

Setting	Description
Source Address Type	Select the type of address from the drop-down list: • **IP Address**. A single IP address. • **IP Network**. A subnet of IP addresses. You need to enter a netmask length in the Mask Length field.
Network Address / IP Address	Depending on your selection of the Source Address Type drop-down list, enter the IP address or the network address.
Mask Length	For a network address, enter the netmask length (0–32). **Note:** By default, a single IP address is assigned a netmask length of 32.

7. Click the **Add** table button. The address is added to the Defined Addresses table.
8. Repeat *step 6* and *step 7* for any other addresses that you want to add to the Defined Addresses table.

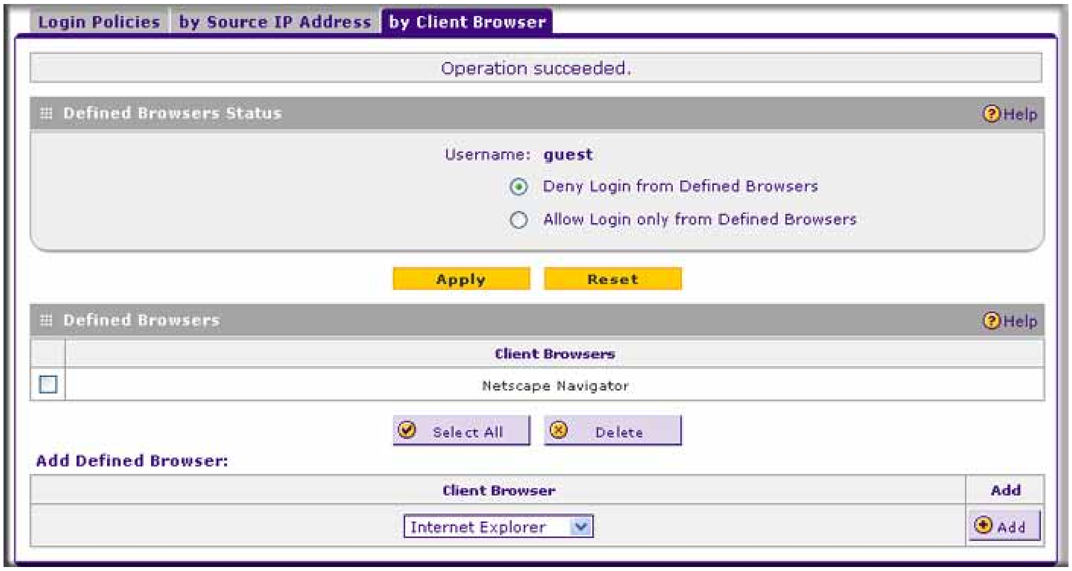
➢ **To delete one or more addresses:**

1. In the Defined Addresses table, select the check box to the left of the address that you want to delete, or click the **Select All** table button to select all addresses.
2. Click the **Delete** table button.

Configure Login Restrictions Based on Web Browser

➢ **To restrict logging in based on the user's browser:**

1. Select **Users > Users**. The Users screen displays (see *Figure 140* on page 227).
2. In the Action column of the List of Users table, click the **Policies** table button for the user for which you want to set login policies. The Policies submenu tabs display, with the Login Policies screen in view.
3. Click the **by Client Browser** submenu tab. The By Client Browser screen displays. (The following figure shows a browser in the Defined Browsers table as an example.)



Operation succeeded.

Username: guest

● Deny Login from Defined Browsers

○ Allow Login only from Defined Browsers

	Client Browsers
□	Netscape Navigator

Add Defined Browser:

Client Browser	Add
Internet Explorer	Add

Figure 144.

4. In the Defined Browsers Status section of the screen, select one of the following radio buttons:
   - **Deny Login from Defined Browsers**. Deny logging in from the browsers in the Defined Browsers table.
   - **Allow Login only from Defined Browsers**. Allow logging in from the browsers in the Defined Browsers table.
5. Click **Apply** to save your settings.
6. In the Add Defined Browser section of the screen, add a browser to the Defined Browsers table by selecting one of the following browsers from the drop-down list:
   - **Internet Explorer**.
   - **Opera**.
   - **Netscape Navigator**.
   - **Firefox**. Mozilla Firefox.
   - **Mozilla**. Other Mozilla browsers.
7. Click the **Add** table button. The browser is added to the Defined Browsers table.
8. Repeat *step 6* and *step 7* for any other browsers that you want to add to the Defined Browsers table.

➢ To delete one or more browsers:

1. In the Defined Browsers table, select the check box to the left of the browser that you want to delete, or click the **Select All** table button to select all browsers.
2. Click the **Delete** table button.

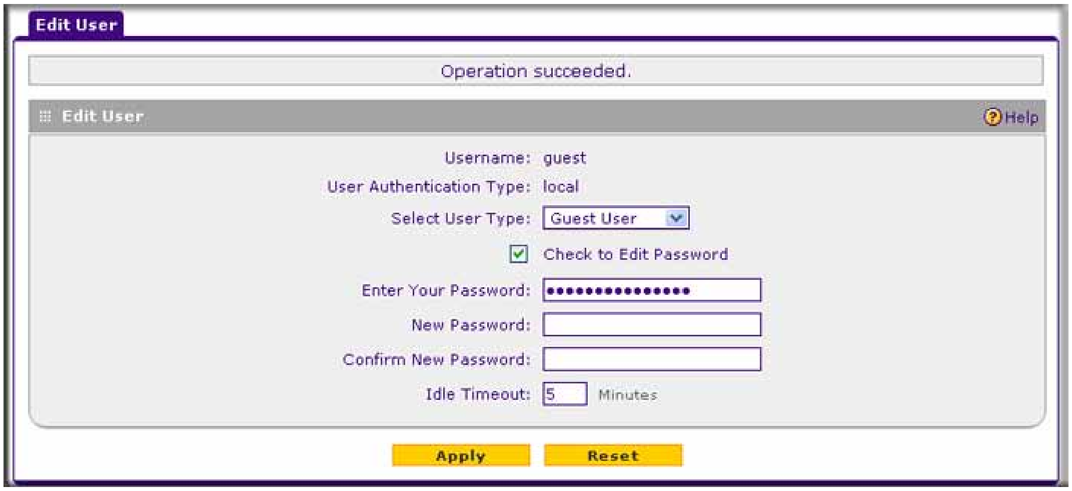
Change Passwords and Other User Settings

For any user, you can change the password, user type, and idle time-out settings. Only administrators have read/write access. All other users have read-only access.

Note: The default password for the administrator and for a guest to access the VPN firewall's web management interface is **password**.

➤ **To modify user settings:**

1. Select **Users > Users**. The Users screen displays (see *Figure 140* on page 227).
2. In the Action column of the List of Users table, click the **Edit** table button for the user for which you want to modify the settings. The Edit User screen displays:



Username: guest
User Authentication Type: local
Select User Type: Guest User
☑ Check to Edit Password
Enter Your Password: •••••••••••••••
New Password:
Confirm New Password:
Idle Timeout: 5 Minutes

Figure 145.

3. Enter the settings as explained in the following table:

Table 60. Edit User screen settings

Setting	Description
User Type	From the drop-down list, select one of the pre-defined user types that determines the access credentials: • **Administrator**. User who has full access and the capacity to change the VPN firewall configuration (that is, read/write access). • **SSL VPN User**. User who can only log in to the SSL VPN portal. • **IPSEC VPN User**. User who can only make an IPSec VPN connection via a NETGEAR ProSafe VPN Client, and only when the XAUTH feature is enabled (see *Configure Extended Authentication (XAUTH)* on page 172). • **Guest User**. User who can only view the VPN firewall configuration (that is, read-only access).

Table 60. Edit User screen settings (continued)

Setting	Description	
Check to Edit Password	Select this check box to make the password fields accessible to modify the password.	
	Enter Your Password	Enter the old password.
	New Password	Enter the new password.
	Confirm New Password	Reenter the new password for confirmation.
Idle Timeout	The period after which an idle user is automatically logged out of the web management interface. De default idle time-out period is 10 minutes.	

4. Click **Apply** to save your settings.

Manage Digital Certificates

The VPN firewall uses digital certificates (also known as X509 certificates) during the Internet Key Exchange (IKE) authentication phase to authenticate connecting IPSec VPN gateways or clients, or to be authenticated by remote entities. The same digital certificates are extended for secure web access connections over HTTPS (that is, SSL connections).

Digital certificates either can be self-signed or can be issued by certification authorities (CAs) such as an internal Windows server or an external organizations such as Verisign or Thawte.

However, if the digital certificate contains the extKeyUsage extension, the certificate needs to be used for one of the purposes defined by the extension. For example, if the digital certificate contains the extKeyUsage extension that is defined for SNMPV2, the same certificate cannot be used for secure web management. The extKeyUsage would govern the certificate acceptance criteria on the VPN firewall when the same digital certificate is being used for secure web management.

On the VPN firewall, the uploaded digital certificate is checked for validity and purpose. The digital certificate is accepted when it passes the validity test and the purpose matches its use. The purpose needs to correspond to its use for IPSec VPN, SSL VPN, or both. If the defined purpose is for IPSec VPN and SSL VPN, the digital certificate is uploaded to both the IPSec VPN certificate repository and the SSL VPN certificate repository. However, if the defined purpose is for IPSec VPN only, the certificate is uploaded only to the IPSec VPN certificate repository.

The VPN firewall uses digital certificates to authenticate connecting VPN gateways or clients, and to be authenticated by remote entities. A digital certificate that authenticates a server, for example, is a file that contains the following elements:

- A public encryption key to be used by clients for encrypting messages to the server.
- Information identifying the operator of the server.
- A digital signature confirming the identity of the operator of the server. Ideally, the signature is from a trusted third party whose identity can be verified.

You can obtain a digital certificate from a well-known commercial certification authority (CA) such as Verisign or Thawte, or you can generate and sign your own digital certificate. Because a commercial CA takes steps to verify the identity of an applicant, a digital certificate from a commercial CA provides a strong assurance of the server's identity. A self-signed certificate triggers a warning from most browsers because it provides no protection against identity theft of the server.

The VPN firewall contains a self-signed certificate from NETGEAR. This certificate can be downloaded from the VPN firewall login screen for browser import. However, NETGEAR recommends that you replace this digital certificate with a digital certificate from a well-known commercial CA prior to deploying the VPN firewall in your network.

Certificates Screen

To display the Certificates screen, select **VPN > Certificates**. Because of the large size of this screen, and because of the way the information is presented, the Certificates screen is divided and presented in this manual in three figures (*Figure 146* on page 236, *Figure 148* on page 238, and *Figure 150* on page 241).

The Certificates screen lets you to view the currently loaded digital certificates, upload a new digital certificate, and generate a certificate signing request (CSR). The VPN firewall typically holds two types of digital certificates:

- **CA digital certificates**. Each CA issues its own CA identity digital certificate to validate communication with the CA and to verify the validity of digital certificates that are signed by the CA.
- **Self-signed certificates**. The digital certificates that are issued to you by a CA to identify your device.

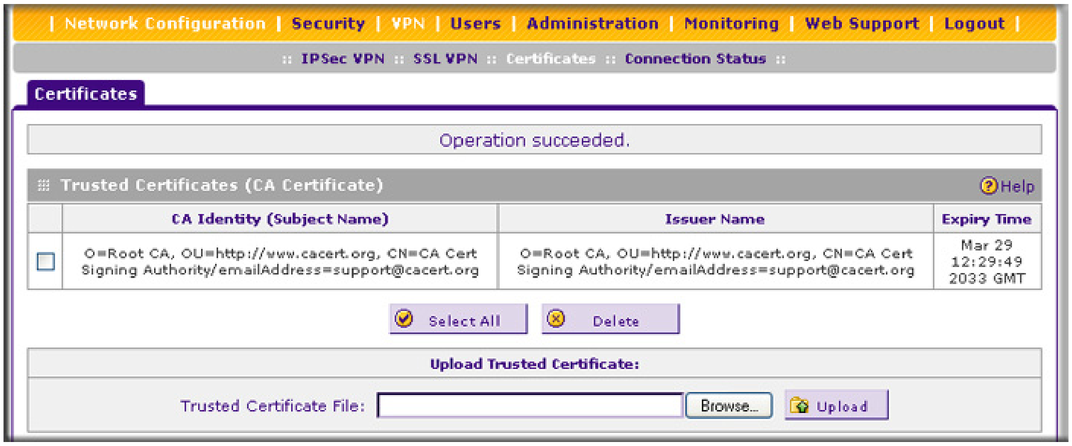
The Certificates screen contains four tables that are explained in detail in the following sections:

- **Trusted Certificates (CA Certificate) table**. Contains the trusted digital certificates that were issued by CAs and that you uploaded (see *Manage Self-Signed Certificates* on page 237).
- **Active Self Certificates table**. Contains the self-signed certificates that were issued by CAs and that you uploaded (see *Manage Self-Signed Certificates* on page 237).
- **Self Certificate Requests table**. Contains the self-signed certificate requests that you generated. These requests might or might not have been submitted to CAs, and CAs might or might not have issued digital certificates for these requests. Only the self-signed certificates in the Active Self Certificates table are active on the VPN firewall (see *Manage Self-Signed Certificates* on page 237).
- **Certificate Revocation Lists (CRL) table**. Contains the lists with digital certificates that have been revoked and are no longer valid, that were issued by CAs, and that you uploaded. Note, however, that the table displays only the active CAs and their critical release date (see *Manage the Certificate Revocation List* on page 241).

Manage CA Certificates

➢ To view and upload trusted certificates:

Select **VPN > Certificates**. The Certificates screen displays. The following figure shows the top section of the screen with the trusted certificate information and one example certificate in the Trusted Certificates (CA Certificate) table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: Certificates :: Connection Status ::
Certificates
Trusted Certificates (CA Certificate)
Help
Select All
Delete
Upload Trusted Certificate:
Trusted Certificate File:
Browse...
Upload

Operation succeeded.

	CA Identity (Subject Name)	Issuer Name	Expiry Time
□	O=Root CA, OU=http://www.cacert.org, CN=CA Cert Signing Authority/emailAddress=support@cacert.org	O=Root CA, OU=http://www.cacert.org, CN=CA Cert Signing Authority/emailAddress=support@cacert.org	Mar 29 12:29:49 2033 GMT

Figure 146. Certificates, screen 1 of 3

The Trusted Certificates (CA Certificate) table lists the digital certificates of CAs and contains the following fields:

- **CA Identity (Subject Name)**. The organization or person to whom the digital certificate is issued.
- **Issuer Name**. The name of the CA that issued the digital certificate.
- **Expiry Time**. The date after which the digital certificate becomes invalid.

➢ To upload a digital certificate of a trusted CA on the VPN firewall:

1. Download a digital certificate file from a trusted CA and store it on your computer.
2. In the Upload Trusted Certificates section of the screen, click **Browse** and navigate to the trusted digital certificate file that you downloaded on your computer.
3. Click the **Upload** table button. If the verification process on the VPN firewall approves the digital certificate for validity and purpose, the digital certificate is added to the Trusted Certificates (CA Certificate) table.

➢ To delete one or more digital certificates:

1. In the Trusted Certificates (CA Certificate) table, select the check box to the left of the digital certificate that you want to delete, or click the **Select All** table button to select all digital certificates.
2. Click the **Delete** table button.

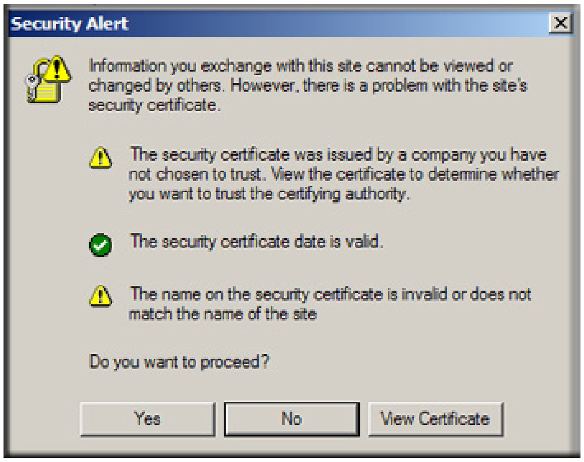
Manage Self-Signed Certificates

Instead of obtaining a digital certificate from a CA, you can generate and sign your own digital certificate. However, a self-signed certificate triggers a warning from most browsers because it provides no protection against identity theft of the server. The following figure shows an image of a browser security alert.

There can be three reasons why a security alert is generated for a security certificate:

- The security certificate was issued by a company you have not chosen to trust.
- The date of the security certificate is invalid.
- The name on the security certificate is invalid or does not match the name of the site.

When a security alert is generated, the user can decide whether or not to trust the host.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

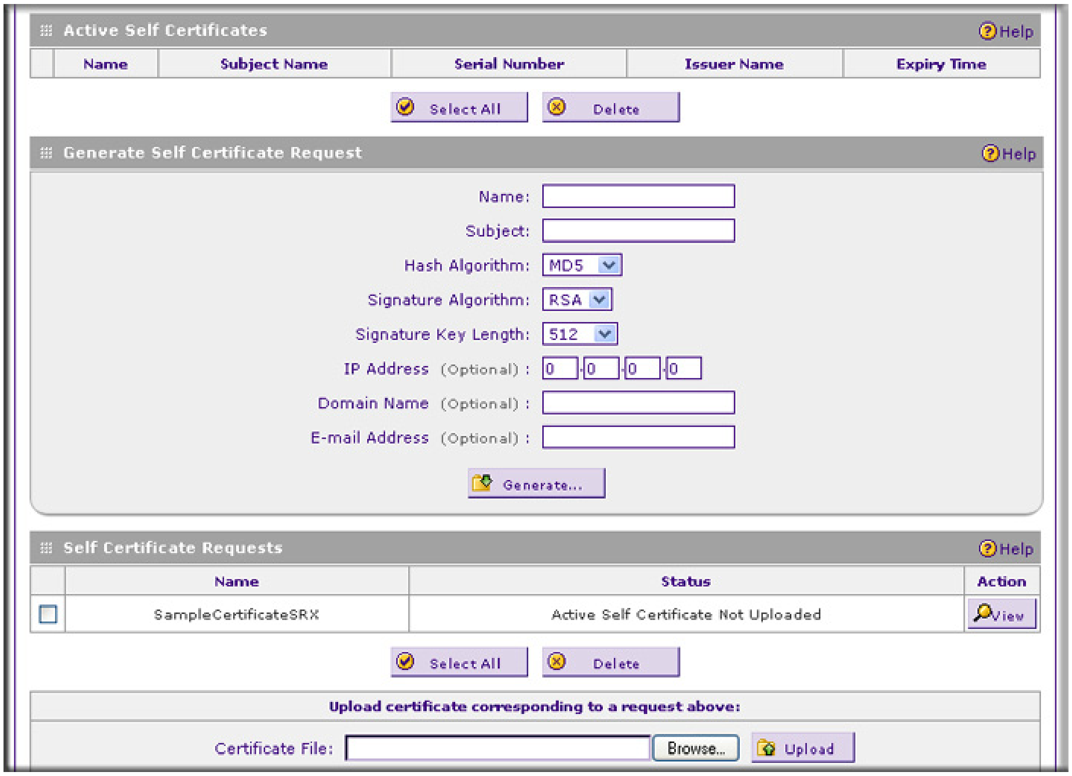
Figure 147.

Generate a CSR and Obtaining a Self-Signed Certificate from a CA

To use a self-signed certificate, you first need to request the digital certificate from a CA, and then download and activate the digital certificate on the VPN firewall. To request a self-signed certificate from a CA, you need to generate a certificate signing request (CSR) for and on the VPN firewall. The CSR is a file that contains information about your company and about the device that holds the certificate. Refer to the CA for guidelines about the information that you need to include in your CSR.

➢ **To generate a new CSR file, obtain a digital certificate from a CA, and upload it to the VPN firewall:**

1. Select **VPN > Certificates**. The Certificates screen displays. The following figure shows the middle section of the screen with the Active Self Certificates section, Generate Self Certificate Request section, and Self Certificate Requests section. (The Self Certificate Requests table contains one example.)



Active Self Certificates

	Name	Subject Name	Serial Number	Issuer Name	Expiry Time

Generate Self Certificate Request

Name:

Subject:

Hash Algorithm: MD5

Signature Algorithm: RSA

Signature Key Length: 512

IP Address (Optional) : 0 . 0 . 0 . 0

Domain Name (Optional) :

E-mail Address (Optional) :

Self Certificate Requests

	Name	Status	Action
□	SampleCertificateSRX	Active Self Certificate Not Uploaded	View

Upload certificate corresponding to a request above:

Certificate File:

Figure 148. Certificates, screen 2 of 3

2. In the Generate Self Certificate Request section of the screen, enter the settings as explained in the following table:

Table 61. Generate self-certificate request settings

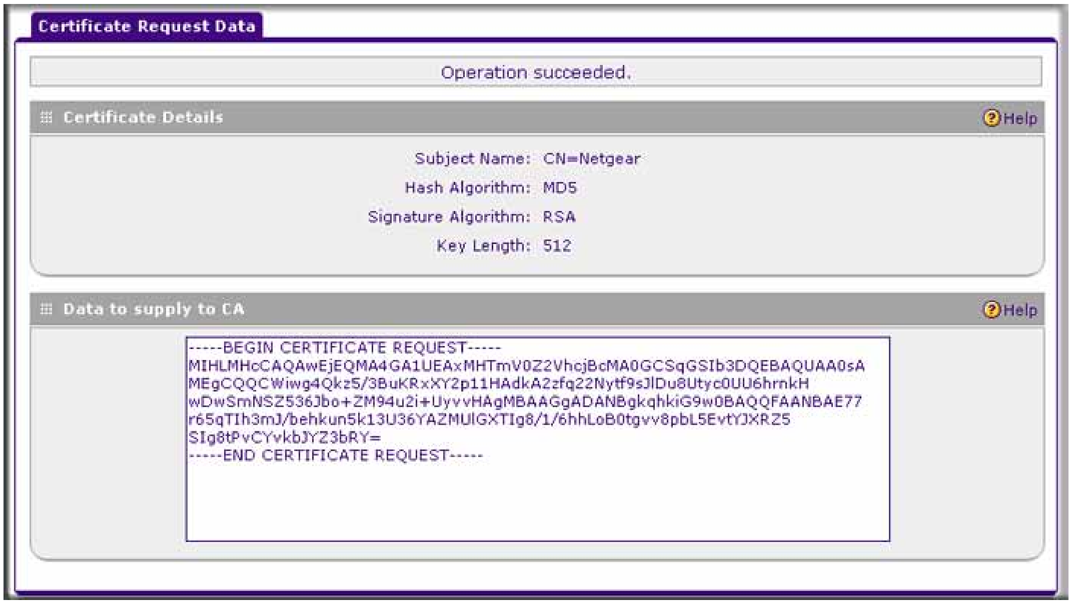
Setting	Description
Name	A descriptive name of the domain for identification and management purposes.
Subject	The name that other organizations see as the holder (owner) of the certificate. In general, use your registered business name or official company name for this purpose. **Note:** Generally, all of your certificates should have the same value in the Subject field.
Hash Algorithm	From the drop-down list, select one of the following hash algorithms: • **MD5**. A 128-bit (16-byte) message digest, slightly faster than SHA-1. • **SHA-1**. A 160-bit (20-byte) message digest, slightly stronger than MD5.
Signature Algorithm	Although this seems to be a drop-down list, the only possible selection is RSA. In other words, RSA is the default to generate a CSR.

Table 61. Generate self-certificate request settings (continued)

Setting	Description	
Signature Key Length	From the drop-down list, select one of the following signature key lengths in bits: • **512** • **1024** • **2048** **Note:** Larger key sizes might improve security, but might also decrease performance.	
Optional Fields	IP Address	Enter your fixed (static) IP address. If your IP address is dynamic, leave this field blank.
	Domain Name	Enter your Internet domain name, or leave this field blank.
	E-mail Address	Enter the email address of a technical contact in your company.

3. Click the **Generate** table button. A new SCR is created and added to the Self Certificate Requests table.

4. In the Self Certificate Requests table, click the **View** table button in the Action column to view the new SCR. The Certificate Request Data screen displays:



Subject Name: CN=Netgear
Hash Algorithm: MD5
Signature Algorithm: RSA
Key Length: 512

```
-----BEGIN CERTIFICATE REQUEST-----
MIHLMHcCAQAwEjEQMA4GA1UEAxMHTmV0Z2VhcjBcMA0GCSqGSIb3DQEBAQUAA0sA
MEgCQQCWiwg4Qkz5/3BuKRxXY2p11HAdkA2zfq22Nytf9sJlDu8Utyc0UU6hrnkH
wDwSmNSZ536Jbo+ZM94u2i+UyvvHAgMBAAGgADANBgkqhkiG9w0BAQQFAANBAE77
r65qTIh3mJ/behkun5k13U36YAZMUlGXTIg8/1/6hhLoB0tgvv8pbL5EvtYJXRZ5
SIg8tPvCYvkbJYZ3bRY=
-----END CERTIFICATE REQUEST-----
```

Figure 149.

5. Copy the contents of the Data to supply to CA text box into a text file, including all of the data contained from “-----BEGIN CERTIFICATE REQUEST-----” to “-----END CERTIFICATE REQUEST-----.”

6. Submit your SCR to a CA:

   a. Connect to the website of the CA.

   b. Start the SCR procedure.

c. When prompted for the requested data, copy the data from your saved text file (including “-----BEGIN CERTIFICATE REQUEST-----” and “-----END CERTIFICATE REQUEST-----”).

d. Submit the CA form. If no problems ensue, the digital certificate is issued by the CA.

7. Download the digital certificate file from the CA and store it on your computer.
8. Return to the Certificates screen (see *Figure 148* on page 238) and locate the Self Certificate Requests section.
9. Select the check box next to the self-signed certificate request.
10. Click **Browse** and navigate to the digital certificate file from the CA that you just stored on your computer.
11. Click the **Upload** table button. If the verification process on the VPN firewall approves the digital certificate for validity and purpose, the digital certificate is added to the Active Self Certificates table.

➢ **To delete one or more SCRs:**

1. In the Self Certificate Requests table, select the check box to the left of the SCR that you want to delete, or click the **Select All** table button to select all SCRs.
2. Click the **Delete** table button.

View and Manage Self-Signed Certificates

The Active Self Certificates table on the Certificates screen (see *Figure 148* on page 238) shows the digital certificates issued to you by a CA and available for use. For each self-signed certificate, the table lists the following information:

- **Name**. The name that you used to identify this digital certificate.
- **Subject Name**. The name that you used for your company and that other organizations see as the holder (owner) of the certificate.
- **Serial Number**. This is a serial number maintained by the CA. It is used to identify the digital certificate with the CA.
- **Issuer Name**. The name of the CA that issued the digital certificate.
- **Expiry Time**. The date on which the digital certificate expires. You should renew the digital certificate before it expires.

➢ **To delete one or more self-signed certificates:**

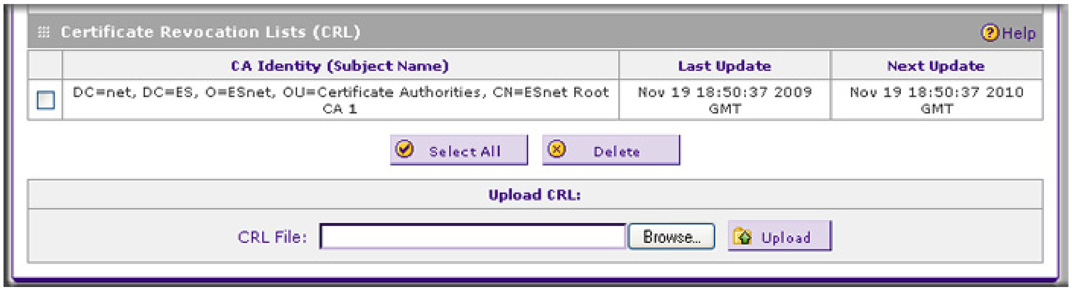
1. In the Active Self Certificates table, select the check box to the left of the self-signed certificate that you want to delete, or click the **Select All** table button to select all self-signed certificates.
2. Click the **Delete** table button.

Manage the Certificate Revocation List

A Certificate Revocation List (CRL) file shows digital certificates that have been revoked and are no longer valid. Each CA issues its own CRLs. It is important that you keep your CRLs up-to-date. You should obtain the CRL for each CA regularly.

➢ To view the currently loaded CRLs and upload a new CRL:

1. Select **VPN > Certificates**. The Certificates screen displays. The following figure shows the bottom section of the screen with the Certificate Revocation Lists (CRL) table. There is one example in the table.



Certificate Revocation Lists (CRL)

	CA Identity (Subject Name)	Last Update	Next Update
□	DC=net, DC=ES, O=ESnet, OU=Certificate Authorities, CN=ESnet Root CA 1	Nov 19 18:50:37 2009 GMT	Nov 19 18:50:37 2010 GMT

Upload CRL:

CRL File:

Figure 150. Certificates, screen 3 of 3

The Certificate Revocation Lists (CRL) table lists the active CAs and their critical release dates:

- **CA Identify (Subject Name)**. The official name of the CA that issued the CRL.
- **Last Update**. The date when the CRL was released.
- **Next Update**. The date when the next CRL will be released.

2. In the Upload CRL section, click **Browse** and navigate to the CLR file that you previously downloaded from a CA.
3. Click the **Upload** table button. If the verification process on the VPN firewall approves the CRL, the CRL is added to the Certificate Revocation Lists (CRL) table.

Note: If the table already contains a CRL from the same CA, the old CRL is deleted when you upload the new CRL.

➢ To delete one or more CRLs:

1. In the Certificate Revocation Lists (CRL) table, select the check box to the left of the CRL that you want to delete, or click the **Select All** table button to select all CRLs.
2. Click the **Delete** table button.

Network and System Management

8

This chapter describes the tools for managing the network traffic to optimize its performance and the system management features of the VPN firewall. This chapter contains the following sections:

- *Performance Management*
- *System Management*

Performance Management

Performance management consists of controlling the traffic through the VPN firewall so that the necessary traffic gets through when there is a bottleneck and either reducing unnecessary traffic or rescheduling some traffic to low-peak times to prevent bottlenecks from occurring in the first place. The VPN firewall has the necessary features and tools to help the network manager accomplish these goals.

Bandwidth Capacity

The maximum bandwidth capacity of the VPN firewall in each direction is as follows:

- LAN side. 4000 Mbps (four LAN ports at 1000 Mbps each)
- WAN side
  - Load balancing mode. 4000 Mbps (four WAN ports at 1000 Mbps each)
  - Auto-rollover mode. 1000 Mbps (one active WAN port at 1000 Mbps)
  - Single-WAN port mode. 1000 Mbps (one active WAN port at 1000 Mbps)

In practice, the WAN side bandwidth capacity is much lower when DSL or cable modems are used to connect to the Internet. At 1.5 Mbps, the WAN ports support the following traffic rates:

- Load balancing mode. 6 Mbps (four WAN ports at 1.5 Mbps each)
- Auto-rollover mode. 1.5 Mbps (one active WAN port at 1.5 Mbps)
- Single WAN port mode. 1.5 Mbps (one active WAN port at 1.5 Mbps)

As a result, and depending on the traffic that is being carried, the WAN side of the VPN firewall is the limiting factor to throughput for most installations.

Using four WAN ports in load balancing mode increases the bandwidth capacity of the WAN side of the VPN firewall, but there is no backup in case one of the WAN ports fails. When such a failure occurs, the traffic that would have been sent on the failed WAN port is diverted to another WAN port that is still working, thus increasing its load. However, there is one exception: Traffic that is bound by protocol to the WAN port that failed is not diverted.

Features That Reduce Traffic

You can adjust the following features of the VPN firewall in such a way that the traffic load on the WAN side decreases:

- LAN WAN outbound rules (also referred to as service blocking)
- DMZ WAN outbound rules (also referred to as service blocking)
- Content filtering
- Source MAC filtering

LAN WAN Outbound Rules and DMZ WAN Outbound Rules (Service Blocking)

You can control specific outbound traffic (from LAN to WAN and from the DMZ to WAN). The LAN WAN Rules screen and the DMZ WAN Rules screen list all existing rules for outbound traffic. If you have not defined any rules, only the default rule is listed. The default rule allows all outgoing traffic. Any outbound rule that you create restricts outgoing traffic and therefore decreases the traffic load on the WAN side.

WARNING!

This feature is for advanced administrators only! Incorrect configuration might cause serious problems.

Each rule lets you specify the desired action for the connections that are covered by the rule:

- BLOCK always
- BLOCK by schedule, otherwise allow
- ALLOW always
- ALLOW by schedule, otherwise block

The following section summarizes the various criteria that you can apply to outbound rules in order to reduce traffic. For more information about outbound rules, see *Outbound Rules (Service Blocking)* on page 83. For detailed procedures on how to configure outbound rules, see *Set LAN WAN Rules* on page 91 and *Set DMZ WAN Rules* on page 95.

When you define outbound firewall rules, you can further refine their application according to the following criteria:

- **Services**. You can specify the services or applications to be covered by an outbound rule. If the desired service or application does not appear in the list, you need to define it on the Services screen (see *Services-Based Rules* on page 83 and *Add Customized Services* on page 112).

- **LAN users**. You can specify which computers on your network are affected by an outbound rule. There are several options:
  - **Any**. The rule applies to all PCs and devices on your LAN.
  - **Single address**. The rule applies to the address of a particular PC.
  - **Address range**. The rule applies to a range of addresses.
  - **Groups**. The rule is applied to a group of PCs. (You can configure groups for LAN WAN outbound rules but not for DMZ WAN outbound rules.) The Known PCs and Devices table is an automatically maintained list of all known PCs and network devices and is generally referred to as the network database, which is described in *Manage the Network Database* on page 68. PCs and network devices are entered into the network database by various methods that are described in *Manage Groups and Hosts (LAN Groups)* on page 67.
- **WAN users**. You can specify which Internet locations are covered by an outbound rule, based on their IP address:
  - **Any**. The rule applies to all Internet IP addresses.
  - **Single address**. The rule applies to a single Internet IP address.
  - **Address range**. The rule applies to a range of Internet IP addresses.
- **Schedule**. You can configure three different schedules to specify when a rule is applied. Once a schedule is configured, it affects all rules that use this schedule. You specify the days of the week and time of day for each schedule. For more information, see *Set a Schedule to Block or Allow Specific Traffic* on page 121.
- **QoS profile**. You can define QoS profiles and then apply them to outbound rules to regulate the priority of traffic. For information about how to define QoS profiles, see *Create Quality of Service (QoS) Profiles* on page 116.
- **Bandwidth profile**. You can define bandwidth profiles and then apply them to outbound rules to limit traffic. For information about how to define bandwidth profiles, see *Create Bandwidth Profiles* on page 118.

Content Filtering

If you want to reduce traffic by preventing access to certain sites on the Internet, you can use the VPN firewall’s content filtering feature. By default, this feature is disabled; all requested traffic from any website is allowed.

- **Web object blocking**. You can block the following web component types: embedded objects (ActiveX, Java, Flash), proxies, and cookies.
- **Keyword and file extension blocking**. You can specify words that, should they appear in the website name (URL), file extension, or newsgroup name, cause that site, file, or newsgroup to be blocked by the VPN firewall.
- **URL blocking**. You can specify URLs that are blocked by the VPN firewall.

For more information, see *Content Filtering* on page 123.

Source MAC Filtering

If you want to reduce outgoing traffic by preventing Internet access by certain PCs on the LAN, you can use the source MAC filtering feature to drop the traffic received from the PCs with the specified MAC addresses. By default, this feature is disabled; all traffic received from PCs with any MAC address is allowed. See *Enable Source MAC Filtering* on page 126 for the procedure on how to use this feature.

Features That Increase Traffic

The following features of the VPN firewall tend to increase the traffic load on the WAN side:

- LAN WAN inbound rules (also referred to as port forwarding)
- DMZ WAN inbound rules (also referred to as port forwarding)
- Port triggering
- Enabling the DMZ port
- Configuring exposed hosts
- Configuring VPN tunnels

LAN WAN Inbound Rules and DMZ WAN Inbound Rules (Port Forwarding)

The LAN WAN Rules screen and the DMZ WAN Rules screen list all existing rules for inbound traffic (from WAN to LAN and from WAN to the DMZ). If you have not defined any rules, only the default rule is listed. The default rule blocks all access from outside except responses to requests from the LAN side. Any inbound rule that you create allows additional incoming traffic and therefore increases the traffic load on the WAN side.

WARNING!

This feature is for advanced administrators only! Incorrect configuration might cause serious problems.

Each rule lets you specify the desired action for the connections covered by the rule:

- BLOCK always
- BLOCK by schedule, otherwise Allow
- ALLOW always
- ALLOW by schedule, otherwise Block

The following section summarizes the various criteria that you can apply to inbound rules and that might increase traffic. For more information about inbound rules, see *Inbound Rules (Port Forwarding)* on page 86. For detailed procedures on how to configure inbound rules, see *Set LAN WAN Rules* on page 91 and *Set DMZ WAN Rules* on page 95.

When you define inbound firewall rules, you can further refine their application according to the following criteria:

- **Services**. You can specify the services or applications to be covered by an inbound rule. If the desired service or application does not appear in the list, you need to define it on the Services screen (see *Services-Based Rules* on page 83 and *Add Customized Services* on page 112).
- **WAN destination IP address**. You can specify the destination IP address for incoming traffic. Traffic is directed to the specified address only when the destination IP address of the incoming packet matches the IP address of the selected WAN interface.
- **LAN users**. You can specify which computers on your network are affected by an inbound rule. There are several options:
  - **Any**. The rule applies to all PCs and devices on your LAN.
  - **Single address**. The rule applies to the address of a particular PC.
  - **Address range**. The rule applies to a range of addresses.
  - **Groups**. The rule is applied to a group of PCs. (You can configure groups for LAN WAN outbound rules but not for DMZ WAN outbound rules.) The Known PCs and Devices table is an automatically maintained list of all known PCs and network devices and is generally referred to as the network database, which is described in *Manage the Network Database* on page 68. PCs and network devices are entered into the network database by various methods that are described in *Manage Groups and Hosts (LAN Groups)* on page 67.
- **WAN users**. You can specify which Internet locations are covered by an inbound rule, based on their IP address:
  - **Any**. The rule applies to all Internet IP addresses.
  - **Single address**. The rule applies to a single Internet IP address.
  - **Address range**. The rule applies to a range of Internet IP addresses.
- **Schedule**. You can configure three different schedules to specify when a rule is applied. Once a schedule is configured, it affects all rules that use this schedule. You specify the days of the week and time of day for each schedule. For more information, see *Set a Schedule to Block or Allow Specific Traffic* on page 121.
- **QoS profile**. You can define QoS profiles and then apply them to inbound rules to regulate the priority of traffic. For information about how to define QoS profiles, see *Create Quality of Service (QoS) Profiles* on page 116.
- **Bandwidth profile**. You can define bandwidth profiles and then apply them to inbound rules to limit traffic. For information about how to define bandwidth profiles, see *Create Bandwidth Profiles* on page 118.

Port Triggering

Port triggering allows some applications running on a LAN network to be available to external applications that would otherwise be partially blocked by the firewall. Using the port triggering feature requires that you know the port numbers used by the application. Without port triggering, the response from the external application would be treated as a new connection request rather than a response to a requests from the LAN network. As such, it would be handled in accordance with the inbound port forwarding rules, and most likely would be blocked.

For the procedure on how to configure port triggering, see *Configure Port Triggering* on page 130.

DMZ Port

The demilitarized zone (DMZ) is a network that, by default, has fewer firewall restrictions when compared to the LAN. The DMZ can be used to host servers (such as a web server, FTP server, or email server) and provide public access to them. The fourth LAN port on the VPN firewall (the rightmost LAN port) can be dedicated as a hardware DMZ port to safely provide services to the Internet without compromising security on your LAN. By default, the DMZ port and both inbound and outbound DMZ traffic are disabled. Enabling the DMZ port and allowing traffic to and from the DMZ increases the traffic through the WAN ports.

For information about how to enable the DMZ port, see *Configure and Enable the DMZ Port* on page 72. For the procedures on how to configure DMZ traffic rules, see *Set DMZ WAN Rules* on page 95.

Exposed Hosts

Specifying an exposed host allows you to set up a computer or server that is available to anyone on the Internet for services that you have not yet defined. For an example of how to set up an exposed host, see *LAN WAN or DMZ WAN Inbound Rule: Specifying an Exposed Host* on page 104.

VPN Tunnels

The VPN firewall supports up to 125 site-to-site IPSec VPN tunnels and up to 50 dedicated SSL VPN tunnels. Each tunnel requires extensive processing for encryption and authentication, thereby increasing traffic through the WAN ports.

For information about IPSec VPN tunnels, see *Chapter 5, Virtual Private Networking Using IPSec Connections*. For information about SSL VPN tunnels, see *Chapter 6, Virtual Private Networking Using SSL Connections*.

Use QoS and Bandwidth Assignment to Shift the Traffic Mix

By specifying QoS and bandwidth profiles and assigning these profiles to outbound and inbound firewall rules, you can shift the traffic mix to aim for optimum performance of the VPN firewall.

Assign QoS Profiles

The QoS profile settings determine the priority and, in turn, the quality of service for the traffic passing through the VPN firewall. After you have created a QoS profile, you can assign the

QoS profile to firewall rules. The QoS is set individually for each service. You can change the mix of traffic through the WAN ports by granting some services a higher priority than others:

- You can accept the default priority defined by the service itself by not changing its QoS setting.
- You can change the priority to a higher or lower value than its default setting to give the service higher or lower priority than it otherwise would have.

For more information about QoS profiles, see *Create Quality of Service (QoS) Profiles* on page 116.

Assigning Bandwidth Profiles

When you apply a QoS profile, the WAN bandwidth does not change. You change the WAN bandwidth that is assigned to a service or application by applying a bandwidth profile. The purpose of bandwidth profiles is to provide a method for allocating and limiting traffic, thus allocating LAN users sufficient bandwidth while preventing them from consuming all the bandwidth on your WAN links.

For more information about bandwidth profiles, see *Create Bandwidth Profiles* on page 118.

Monitoring Tools for Traffic Management

The VPN firewall includes several tools that can be used to monitor the traffic conditions of the firewall and content filtering engine and to monitor the users' access to the Internet and the types of traffic that they are allowed to have. See *Chapter 9, Monitoring System Access and Performance* for a description of these tools.

System Management

System management tasks are described in the following sections:

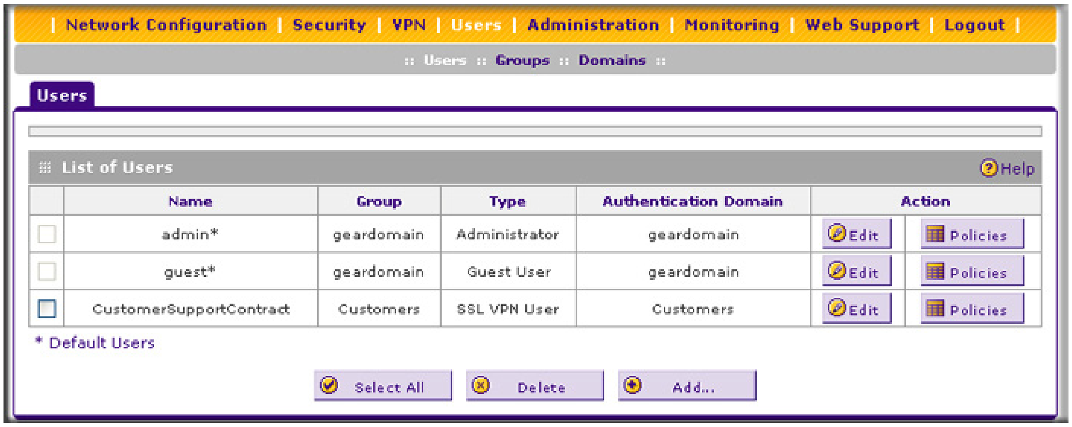
- *Change Passwords and Administrator Settings*
- *Configure Remote Management Access*
- *Using the Command-Line Interface*
- *Use a Simple Network Management Protocol Manager*
- *Manage the Configuration File*
- *Configure Date and Time Service*

Change Passwords and Administrator Settings

The default administrator and default guest passwords for the web management interface are both **password**. NETGEAR recommends that you change the password for the administrator account to a more secure password, and that you configure a separate secure password for the guest account.

➢ To modify the administrator user account settings, including the password:

1. Select **Users > Users**. The Users screen displays. The following figure shows the VPN firewall’s default users—admin and guest—and, as an example, one other user in the List of Users table.

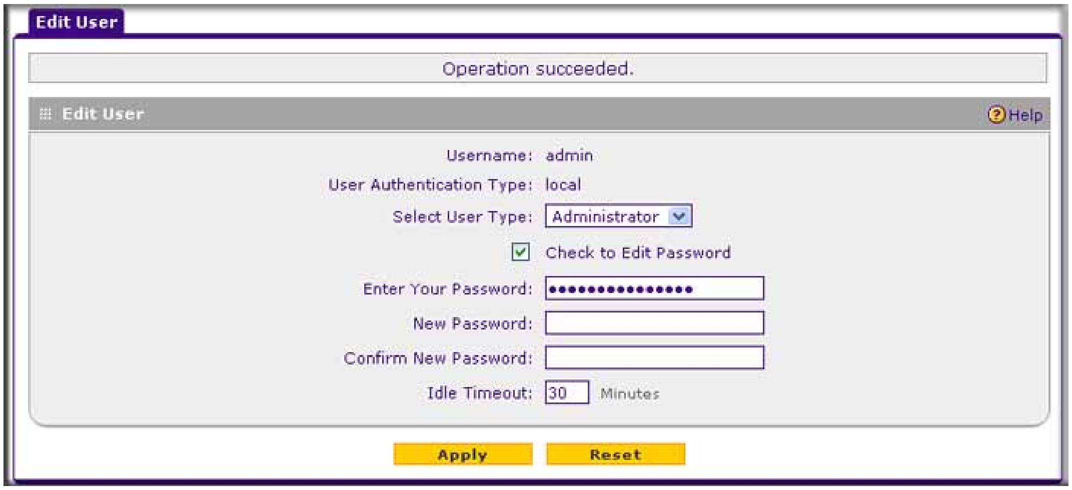

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Users :: Groups :: Domains ::
Users
List of Users
Help
Select All
Delete
Add...

	Name	Group	Type	Authentication Domain	Action	
□	admin*	geardomain	Administrator	geardomain	Edit	Policies
□	guest*	geardomain	Guest User	geardomain	Edit	Policies
□	CustomerSupportContract	Customers	SSL VPN User	Customers	Edit	Policies

* Default Users

Figure 151.

2. In the Action column of the List of Users table, click the **Edit** table button for the user with the name admin. The Edit User screen displays:



Operation succeeded.

Username:	admin
User Authentication Type:	local
Select User Type:	Administrator
☑	Check to Edit Password
Enter Your Password:	●●●●●●●●●●●●●●●
New Password:	
Confirm New Password:	
Idle Timeout:	30 Minutes

Figure 152.

3. Select the **Check to Edit Password** check box. The password fields become available.
4. Enter the old password, enter the new password, and then confirm the new password.

Note: The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both uppercase and lowercase), numbers, and symbols. Your password can be up to 30 characters.

5. As an option, you can change the idle time-out for an administrator login session. Enter a new number of minutes in the Idle Timeout field. (The default setting is 5 minutes.)
6. Click **Apply** to save your settings.
7. Repeat *step 1* through *step 6* for the user with the name guest.

Note: After a factory default reset, the password and time-out value are changed back to **password** and 5 minutes, respectively.

You can also change the administrator login policies:

- Deny login access from a WAN interface. By default, the administrator can log in from a WAN interface.
- Deny or allow login access from specific IP addresses. By default, the administrator can log in from any IP address.

Note: For enhanced security, restrict access to as few external IP addresses as practical.

- Deny or allow login access from specific browsers. By default, the administrator can log in from any browser.

In general, these policy settings work well for an administrator. However, if you need to change any of these policy settings, see *Set User Login Policies* on page 229.

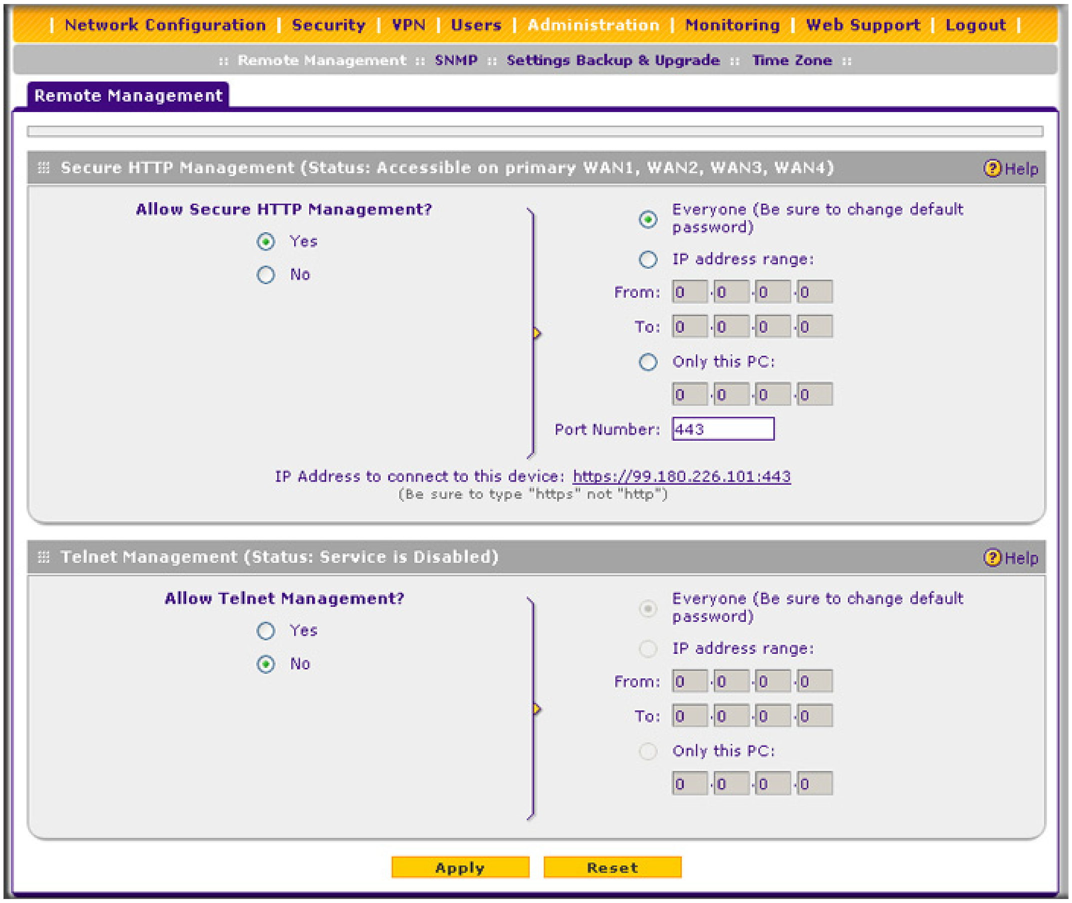
Configure Remote Management Access

An administrator can configure, upgrade, and check the status of the VPN firewall over the Internet through either a Secure Sockets Layer (SSL) VPN or a Telnet connection, but need to be logged in locally to enable remote management.

Note: When remote management is enabled and administrative access through a WAN interface is granted (see *Configure Login Policies* on page 229), the VPN firewall's web management interface is accessible to anyone who knows its IP address and default password. Because a malicious WAN user can reconfigure the VPN firewall and misuse it in many ways, NETGEAR highly recommends that you change the admin and guest default passwords before continuing (see *Change Passwords and Administrator Settings* on page 248).

➤ To configure the VPN firewall for remote management:

1. Select **Administration > Remote Management**. The Remote Management screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone ::
Remote Management
Help
Help
Apply
Reset

Secure HTTP Management (Status: Accessible on primary WAN1, WAN2, WAN3, WAN4)

Allow Secure HTTP Management?

● Yes

○ No

● Everyone (Be sure to change default password)

○ IP address range:

From: 0 . 0 . 0 . 0

To: 0 . 0 . 0 . 0

○ Only this PC:

0 . 0 . 0 . 0

Port Number: 443

IP Address to connect to this device: https://99.180.226.101:443
(Be sure to type "https" not "http")

Telnet Management (Status: Service is Disabled)

Allow Telnet Management?

○ Yes

● No

● Everyone (Be sure to change default password)

○ IP address range:

From: 0 . 0 . 0 . 0

To: 0 . 0 . 0 . 0

○ Only this PC:

0 . 0 . 0 . 0

Figure 153.

2. Enter the settings as explained in the following table:

Table 62. Remote Management screen settings

<table>
<tr><th>Setting</th><th colspan="2">Description</th></tr>
<tr><td colspan="3"><b>Secure HTTP Management</b></td></tr>
<tr><td rowspan="3">Allow Secure HTTP Management?
<b>Note:</b> The IP address and port number to connect to the VPN firewall are shown in this section of the screen.</td><td colspan="2">Select the <b>Yes</b> radio button to enable HTTPS remote management (which is the default setting) and specify the IP address settings and port number settings. Select the <b>No</b> radio button to disable HTTPS remote management.</td></tr>
<tr><td colspan="2">Select one of the following IP address settings:
• <b>Everyone</b>. Allow access from any IP address on the Internet.
• <b>IP address range</b>. Allow access from a range of IP addresses on the Internet. Enter a beginning and ending IP address to define the allowed range.
• <b>Only this PC</b>. Allow access from a single IP address on the Internet. Enter a single IP address.</td></tr>
<tr><td>Port Number</td><td>The default HTTPS port is 443. As an option, you can change the port number.</td></tr>
<tr><td rowspan="2">Telnet Management</td><td colspan="2">Select the <b>Yes</b> radio button to enable Telnet remote management and specify the IP address settings. Select the <b>No</b> radio button to disable HTTPS remote management (which is the default setting).</td></tr>
<tr><td colspan="2">Select one of the following IP address settings:
• <b>Everyone</b>. Allow access from any IP address on the Internet.
• <b>IP address range</b>. Allow access from a range of IP addresses on the Internet. Enter a beginning and ending IP address to define the allowed range.
• <b>Only this PC</b>. Allow access from a single IP address on the Internet. Enter a single IP address.</td></tr>
</table>

3. Click **Apply** to save your changes.

WARNING!

If you are remotely connected to the VPN firewall and you select the No radio button to disable HTTP remote management, you and all other SSL VPN users are disconnected when you click Apply.

When remote management is enabled, you need to use an SSL connection to access the VPN firewall from the Internet. You need to enter https:// (not http://) and type the VPN firewall's WAN IP address in your browser. For example, if the VPN firewall's WAN IP address is 172.16.0.123, type the following in your browser: **https://172.16.0.123**.

The VPN firewall's remote login URL is:

https://<IP_address> or https://<FullyQualifiedDomainName>

Note: For enhanced security, and if practical, restrict remote management access to a single IP address or a small range of IP addresses.

Note: To maintain security, the VPN firewall rejects a login that uses *http://address* rather than the SSL *https://address*.

Note: The first time that you remotely connect to the VPN firewall with a browser via an SSL connection, you might get a warning message regarding the SSL certificate. If you are using a Windows computer with Internet Explorer 5.5 or later, simply click Yes to accept the certificate.

Note: If you are unable to remotely connect to the VPN firewall after enabling HTTPS remote management, check if other user policies, such as the default user policy, are preventing access. For access to the VPN firewall’s web management interface, check if administrative access through a WAN interface is granted (see *Configure Login Policies* on page 229).

Note: If you disable HTTPS remote management, all SSL VPN user connections are also disabled.

Tip: If you are using a dynamic DNS service such as TZO, you can identify the WAN IP address of your VPN firewall by running `tracert` from the Windows Run menu option. Trace the route to your registered FQDN. For example, enter **`tracert VPN firewall.mynetgear.net`**, and the WAN IP address that your ISP assigned to the VPN firewall is displayed.

Using the Command-Line Interface

You can access the command-line interface (CLI) using the console port on the rear panel of the VPN firewall (see *Rear Panel* on page 16).

You can access the CLI from a communications terminal when the VPN firewall is still set to its factory defaults (or use your own settings if you have changed them).

➤ **To access the CLI:**

1. From your computer’s command-line prompt, enter the following command:

```
telnet 192.168.1.1
```

2. Enter **`admin`** and **`password`** when prompted for the login and password information (or enter **`guest`** and **`password`** to log in as a read-only guest).
3. Enter **`exit`** to end the CLI session.

Any configuration changes made via the CLI are not preserved after a reboot or power cycle unless you issue the CLI **`save`** command after making the changes.

Use a Simple Network Management Protocol Manager

Simple Network Management Protocol (SNMP) forms part of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

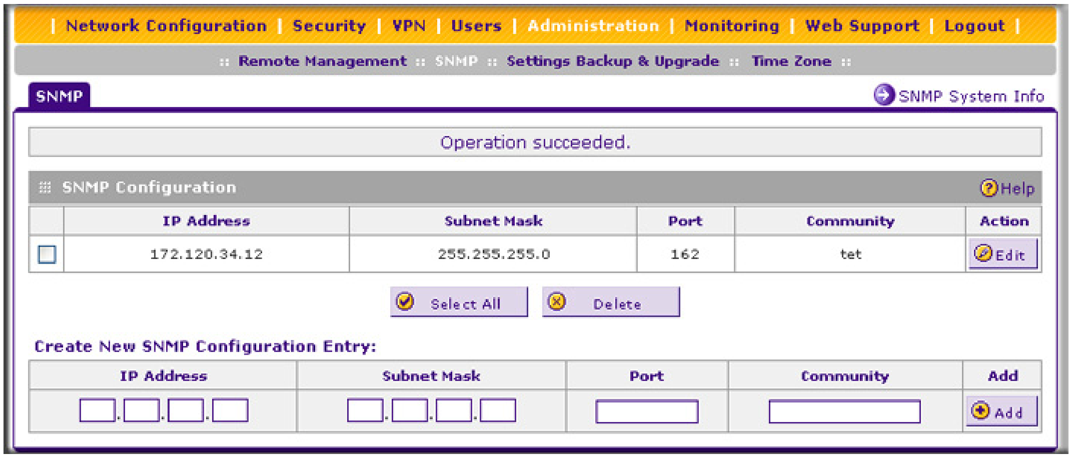
SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

SNMP lets you monitor and manage your VPN firewall from an SNMP manager. It provides a remote means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

Manage the SNMP Configuration

➤ **To create a new SNMP configuration entry:**

1. Select **Administration > SNMP**. The SNMP screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone ::
SNMP
SNMP System Info
Help
Select All
Delete
Edit
Add

Operation succeeded.

SNMP Configuration

	IP Address	Subnet Mask	Port	Community	Action
□	172.120.34.12	255.255.255.0	162	tet	Edit

Create New SNMP Configuration Entry:

IP Address	Subnet Mask	Port	Community	Add
. . .	. . .			Add

Figure 154.

2. In the Create New SNMP Configuration Entry section of the screen, enter the settings as explained in the following table:

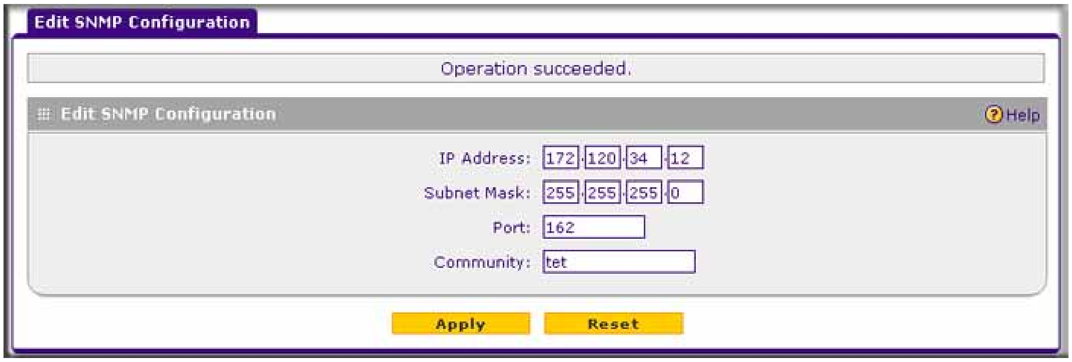
Table 63. SNMP screen settings

Setting	Description
IP Address	The IP addresses of the SNMP management station that is allowed to receive the VPN firewall's SNMP traps.
Subnet Mask	The subnet mask of the SNMP management station that is allowed to receive the VPN firewall's SNMP traps. To allow a subnet access to the VPN firewall through SNMP, enter a subnet mask of 255.255.255.0. In this situation, the entire subnet that is associated with the IP address of the SNMP management station has access through the community string. **Note:** A subnet mask of 255.255.255.255 or 0.0.0.0 is not supported.
Port	The SNMP trap port of the SNMP manager that is allowed to receive the VPN firewall's SNMP traps. The default port number is 162.
Community	The community string to which the SNMP agent belongs.

3. Click the **Add** table button. The SNMP configuration is added to the SNMP Configuration table.

➢ To edit an SNMP configuration:

1. On the SNMP screen (see the previous figure), click the **Edit** button in the Action column for the SNMP configuration that you want to modify. The Edit SNMP Configuration screen displays.



Operation succeeded.

IP Address: 172 . 120 . 34 . 12
Subnet Mask: 255 . 255 . 255 . 0
Port: 162
Community: tet

Figure 155.

2. Modify the settings as explained in the previous table.
3. Click **Apply** to save your settings.

➢ To delete one or more SNMP configuration entries:

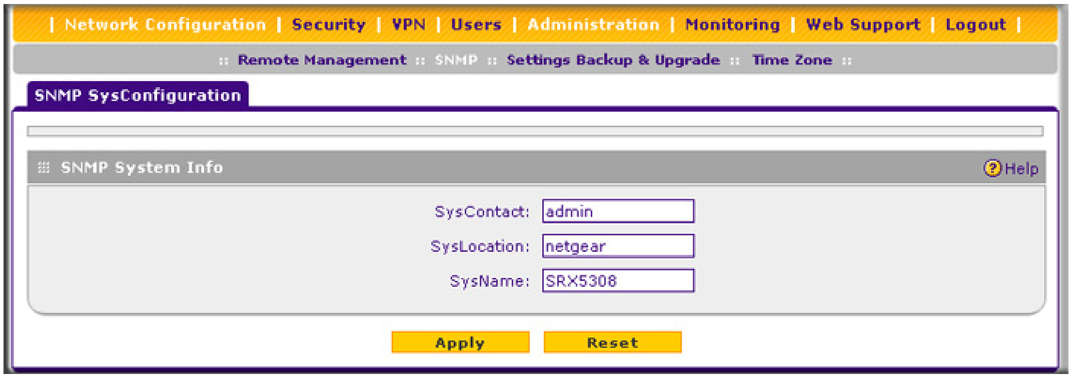
1. On the SNMP screen (see *Figure 154* on page 254), select the check box to the left of the SNMP configuration that you want to delete, or click the **Select All** table button to select all SNMP configurations.
2. Click the **Delete** table button.

Manage the VPN Firewall's SNMP System Information

The following VPN firewall identification information is available to an SNMP manager: system contact, system location, and system name.

➤ **To modify the SNMP identification information:**

1. Select **Administration > SNMP**. The SNMP screen displays (see *Figure 154* on page 254).
2. Click the **SNMP System Info** option arrow in the upper right of the screen link. The SNMP SysConfiguration screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone ::
SNMP SysConfiguration
SNMP System Info
Help
Apply
Reset

SysContact: admin

SysLocation: netgear

SysName: SRX5308

Figure 156.

3. Modify any of the information that you want the SNMP manager to use. You can edit the system contact, system location, and system name.
4. Click **Apply** to save your settings.

Manage the Configuration File

The configuration settings of the VPN firewall are stored in a configuration file on the VPN firewall. This file can be saved (backed up) to a PC, retrieved (restored) from the PC, or cleared to factory default settings.

Once the VPN firewall is installed and works correctly, make a backup of the configuration file to a computer. If necessary, you can later restore the VPN firewall settings from this file.

The Settings Backup and Firmware Upgrade screen lets you do the following:

- Back up and save a copy of the current settings.
- Restore saved settings from the backed-up file.
- Revert to the factory default settings.
- Upgrade the VPN firewall firmware from a saved file on your hard disk to use a different firmware version.

➤ To display the Settings Backup and Firmware Upgrade screen:

Select **Administration > Settings Backup and Firmware Upgrade**.

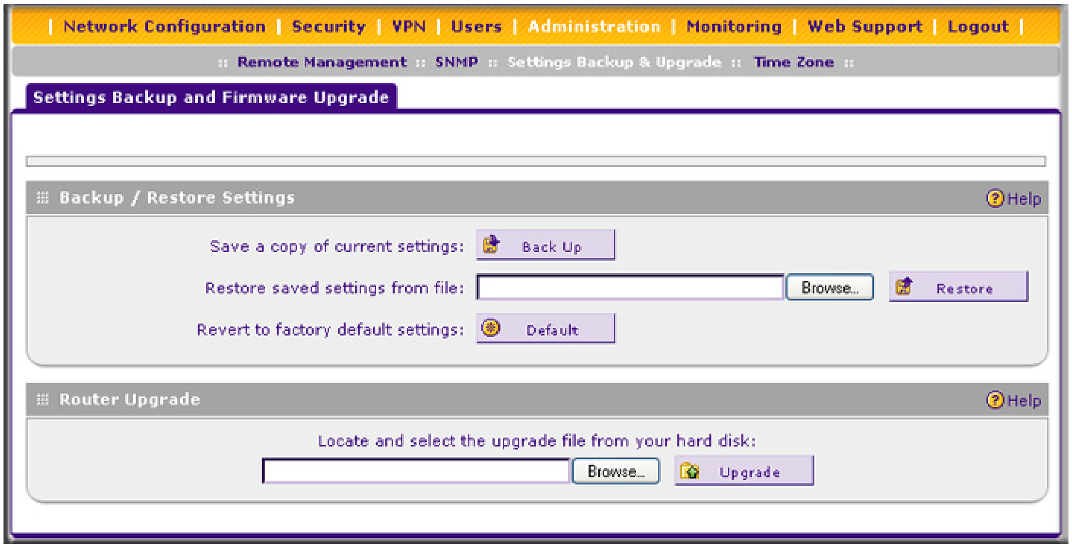

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone ::
Settings Backup and Firmware Upgrade
Backup / Restore Settings
Help
Save a copy of current settings:
Back Up
Restore saved settings from file:
Browse...
Restore
Revert to factory default settings:
Default
Router Upgrade
Help
Locate and select the upgrade file from your hard disk:
Browse...
Upgrade

Figure 157.

Back Up Settings

The backup feature saves all VPN firewall settings to a file. These settings include the IP addresses, subnet masks, gateway addresses, and so on.

Back up your VPN firewall settings periodically, and store the backup file in a safe place.

> **Tip:** You can use a backup file to export all settings to another VPN firewall that has the same language and management software versions. Remember to change the IP address of the second VPN firewall before deploying it to eliminate IP address conflicts on the network.

➤ To back up settings:

1. On the Settings Backup and Firmware Upgrade screen (see the previous screen), next to Save a copy of current settings, click the **Back Up** button to save a copy of your current settings. A warning appears, and then a screen, showing the file name of the backup file (SRX5308.cfg).
2. Select **Save file**, and then click **OK**.
3. Open the folder where you have saved the backup file, and then verify that it has been saved successfully.

Note the following:

- If your browser is not configured to save downloaded files automatically, locate the folder in which you want to save the file, specify the file name, and save the file.
- If your browser is configured to save downloaded files automatically, the file is saved to your browser’s download location on the hard disk.

Restore Settings

WARNING!

Restore only settings that were backed up from the same software version. Restoring settings from a different software version can corrupt your backup file or the VPN firewall system software.

➤ **To restore settings from a backup file:**

1. On the Settings Backup and Firmware Upgrade screen (see the previous screen), next to Restore saved settings from file, click **Browse**.
2. Locate and select the previously saved backup file (by default, SRX5308.cfg).
3. After you have selected the file, click the **Restore** button. A warning message might appear, and you might have to confirm that you want to restore the configuration.

The VPN firewall reboots. An alert message appears indicating the status of the restore operation. You need to manually restart the VPN firewall for the restored settings to take effect.

WARNING!

Once you start restoring settings, do *not* interrupt the process. Do not try to go online, turn off the VPN firewall, shut down the computer, or do anything else to the VPN firewall until the settings have been fully restored.

Revert to Factory Default Settings

➤ **To reset the VPN firewall to the original factory default settings, you can use one of the following two methods:**

- Using a sharp object, press and hold the reset button on the rear panel of the VPN firewall (see *Rear Panel* on page 16) for about eight seconds until the Test LED turns on. The Test LED remains on for about 2 minutes. To restore the factory default configuration settings when you do not know the administration password or IP address, you need to use the reset button method.
- On the Settings Backup and Firmware Upgrade screen (see the previous screen), next to Revert to factory default settings, click the **Default** button.

The VPN firewall reboots. The reboot process is complete after several minutes when the Test LED on the front panel goes off.

⚠ **WARNING!**

When you push the hardware reset button or click the software Default button, the VPN firewall settings are erased. All firewall rules, VPN policies, LAN/WAN settings, and other settings are lost. Back up your settings if you intend on using them.

Note: After rebooting with factory default settings, the VPN firewall's password is **password** and the LAN IP address is **192.168.1.1**.

Upgrade the Firmware and Reboot the VPN Firewall

You can install a different version of the VPN firewall firmware from the Settings Backup and Firmware Upgrade screen (see the previous screen). To view the current version of the firmware that your VPN firewall is running, select **Monitoring** from the main navigation menu. The Router Status screen displays, showing the firmware version in the System Info section of the screen. After you have upgraded the firmware, the new firmware version is shown on the screen.

➤ **To download a firmware version and upgrade the VPN firewall:**

1. Go to the NETGEAR website at *http://www.netgear.com/support*:
   a. Under Find Your Product, enter SRX5308, and then click on the product number. The SRX5308 support screen displays.
   b. Click the orange Downloads tab.
   c. Click the desired firmware version to reach the download page. Be sure to read the release notes on the download page before upgrading the VPN firewall's software.
2. Download the firmware file to your computer. Note the following:
   - If your browser is not configured to save downloaded files automatically, locate the folder in which you want to save the file, specify the file name, and save the file.
   - If your browser is configured to save downloaded files automatically, the file is saved to your browser's download location on the hard disk.
3. Select **Administration > Settings Backup and Firmware Upgrade**. The Settings Backup and Firmware Upgrade screen displays (see the previous screen).
4. In the Router Upgrade section of the screen, click the **Browse** button.
5. Locate and select the firmware file that you have downloaded.
6. After you have selected the file, click the **Upload** button to start the software upgrade to your VPN firewall. The upgrade process might take some time, at the conclusion of which the VPN firewall reboots automatically. The reboot process is complete after several minutes when the Test LED on the front panel goes off.

WARNING!

Do not try to go online, turn off the VPN firewall, shut down the computer or do anything else to the VPN firewall until the VPN firewall finishes the upgrade! When the Test light turns off, wait a few more seconds before doing anything.

7. After the VPN firewall has completed its reboot process, log in to the web management interface, click **Monitoring** to display the Router Status screen, and then verify that the VPN firewall has the new software installed.

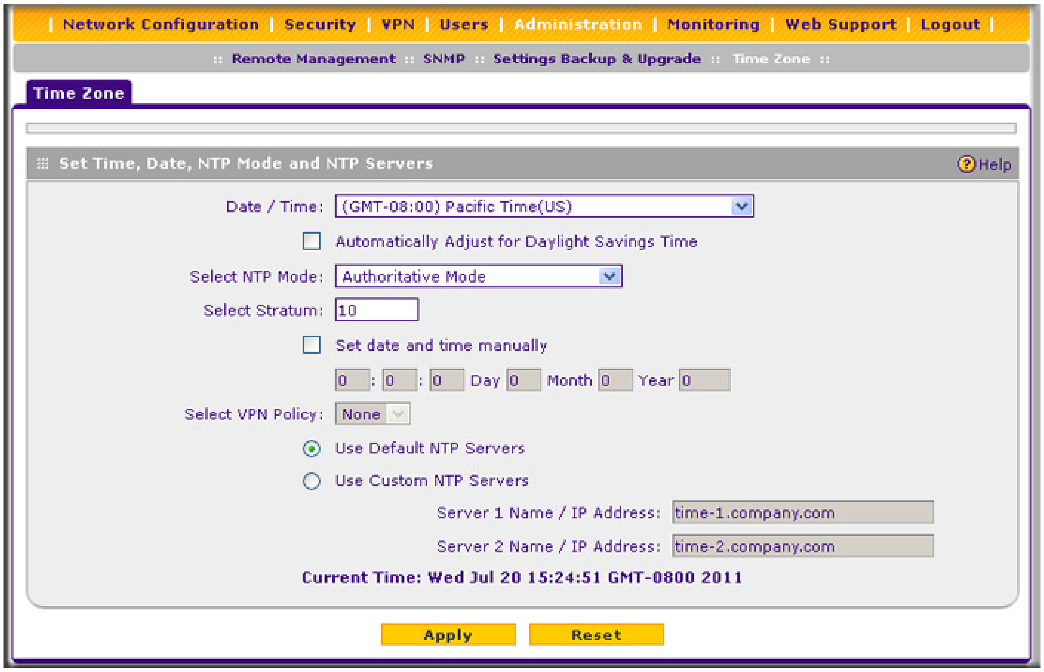
Note: In some cases, such as a major upgrade, it might be necessary to erase the configuration and manually reconfigure your VPN firewall after upgrading it. Refer to the release notes included with the software to find out if this is required.

Configure Date and Time Service

Configure date, time, and NTP server designations on the Time Zone screen. Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock times in a network of computers. Setting the correct system time and time zone ensures that the date and time recorded in the VPN firewall logs and reports are accurate.

➤ **To set time, date, and NTP servers:**

1. Select **Administration > Time Zone**. The Time Zone screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone ::
Time Zone
Set Time, Date, NTP Mode and NTP Servers
Help
Apply
Reset

Date / Time: (GMT-08:00) Pacific Time(US)

□ Automatically Adjust for Daylight Savings Time

Select NTP Mode: Authoritative Mode

Select Stratum: 10

□ Set date and time manually

0 : 0 : 0 Day 0 Month 0 Year 0

Select VPN Policy: None

● Use Default NTP Servers

○ Use Custom NTP Servers

Server 1 Name / IP Address: time-1.company.com

Server 2 Name / IP Address: time-2.company.com

Current Time: Wed Jul 20 15:24:51 GMT-0800 2011

Figure 158.

The bottom of the screen displays the current weekday, date, time, time zone, and year (in the example in the previous figure: Current Time: Wed Jul 2015:24:51 GMT-0800 2011).

2. Enter the settings as explained in the following table:

Table 64. Time Zone screen settings

Setting	Description	
Date/Time	From the drop-down list, select the local time zone in which the VPN firewall operates. The correct time zone is required in order for scheduling to work correctly. The VPN firewall includes a real-time clock (RTC), which it uses for scheduling.	
Automatically Adjust for Daylight Savings Time	If daylight savings time is supported in your region, select the **Automatically Adjust for Daylight Savings Time** check box.	
Select NTP Mode	In all three NTP modes, the VPN firewall functions both as a client and a server. The VPN firewall synchronizes its clock with the specified NTP server or servers and provides time service to clients. From the drop-down list, select the NTP mode: • **Authorative Mode**. The VPN firewall synchronizes its clock with the specified NTP server or servers on the Internet. If external servers are unreachable, the VPN firewall's RTC provides time service to clients. In authorative mode, you can enter a stratum value and set the date and time manually. • **Sync to NTP Servers on Internet**. The VPN firewall synchronizes its clock with the specified NTP server or servers on the Internet. If external servers are unreachable, the VPN firewall does *not* use it's RTC. • **Sync to NTP Servers on VPN**. The VPN firewall synchronizes its clock with the specified NTP server on the VPN. If the server is unreachable, the VPN firewall does *not* use it's RTC. You need to select a VPN policy that enables the VPN firewall to contact the NTP server on the VPN.	
	Select Stratum	In authorative mode, enter a stratum value, which indicates the distance from a reference clock. The default value is 10, which specifies an unsynchronized local clock and causes NTP to use the VPN firewall's RTC when the specified NTP server is not available.
	Set date and time manually	This is an optional setting that is available in authorative mode. Select the check box to unmask the time (hour, minute, second), Day, Month, and Year fields. Enter the date and time.
	Select VPN Policy	When the VPN firewall is configured to synchronize to an NTP server on the VPN, select the VPN policy from the drop-down list. For information about configuring VPN policies, see *Configure VPN Policies* on page 165.

Table 64. Time Zone screen settings (continued)

Setting	Description	
NTP Server (default or custom)	From the drop-down list, select an NTP server: • **Use Default NTP Servers**. The VPN firewall's RTC is updated regularly by contacting a default NETGEAR NTP server on the Internet. • **Use Custom NTP Servers**. The VPN firewall's RTC is updated regularly by contacting one of the two NTP servers (primary and backup), both of which you need to specify in the fields that become available with this menu selection. **Note:** If you select this option but leave either the Server 1 or Server 2 field blank, both fields are set to the default NETGEAR NTP servers. **Note:** A list of public NTP servers is available at *http://ntp.isc.org/bin/view/Servers/WebHome*.	
	Server 1 Name / IP Address	Enter the IP address or host name the primary NTP server.
	Server 2 Name / IP Address	Enter the IP address or host name the backup NTP server.

3. Click **Apply** to save your settings.

Note: If you select the default NTP servers or if you enter a custom server FQDN, the VPN firewall determines the IP address of the NTP server by performing a DNS lookup. You need to configure a DNS server address on a WAN ISP Settings screen (see *Manually Configure the Internet Connection* on page 28) before the VPN firewall can perform this lookup.

9. Monitoring System Access and Performance

9

This chapter describes the system monitoring features of the VPN firewall. You can be alerted to important events such as changes in WAN port status, WAN traffic limits reached, hacker probes and login attempts, dropped packets, and more. You can also view status information about the firewall, WAN ports, LAN ports, active VPN users and tunnels, and more. In addition, the diagnostics utilities are described.

> **Note:** To receive logs by email, you need to configure the email notification server—see *Activate Notification of Events, Alerts, and Syslogs* on page 269.

This chapter contains the following sections:

- *Enable the WAN Traffic Meter*
- *Enable the LAN Traffic Meter*
- *Activate Notification of Events, Alerts, and Syslogs*
- *View Status and Log Screens*
- *Use the Diagnostics Utilities*

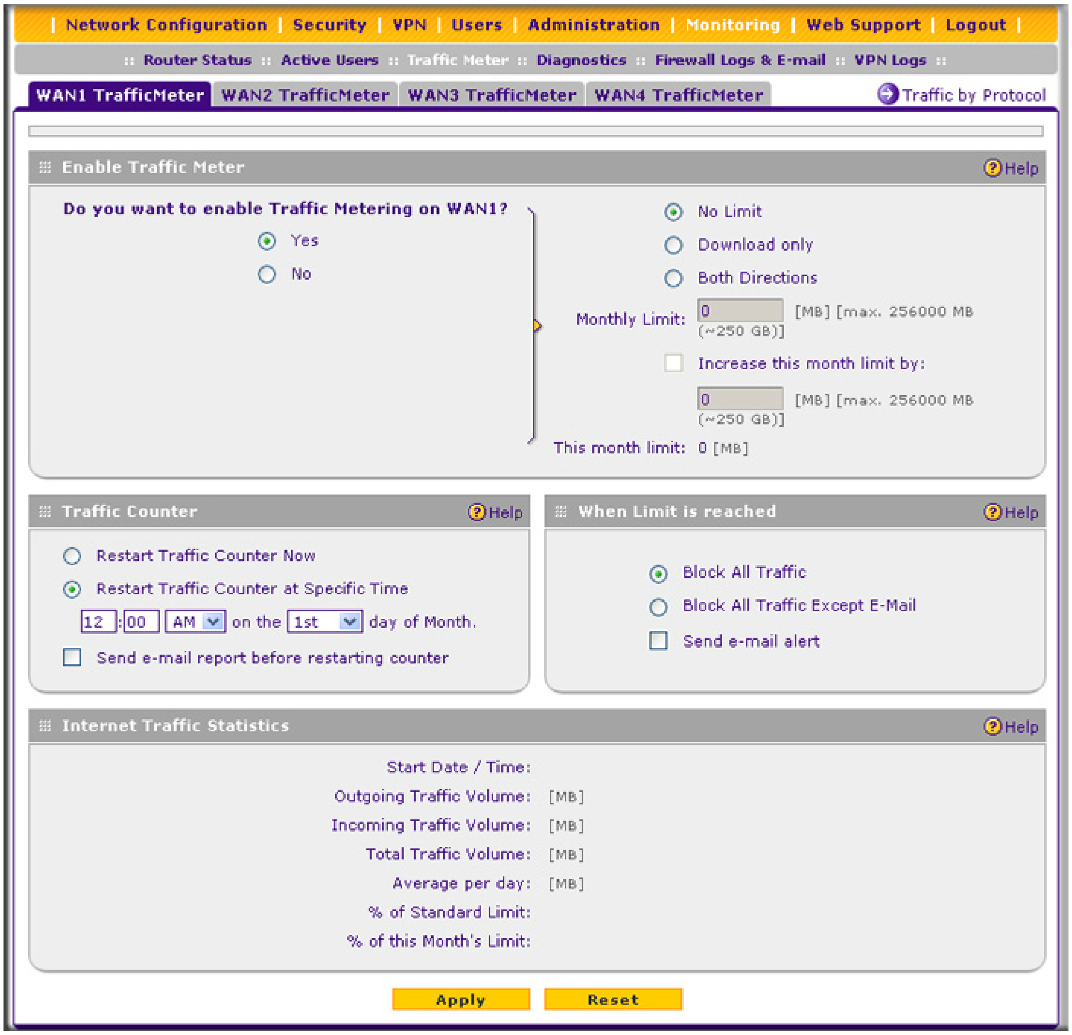
Enable the WAN Traffic Meter

If your ISP charges by traffic volume over a given period of time, or if you want to study traffic types over a period of time, you can activate the traffic meter for one or more WAN ports.

➤ **To monitor traffic limits on each of the WAN ports:**

1. Select **Monitoring > Traffic Meter**. The WAN Traffic Meter tabs display, with the WAN1 Traffic Meter screen in view (see the following figure).

   The Internet Traffic Statistics section in the lower part of the screen displays statistics on Internet traffic via the WAN port. If you have not enabled the traffic meter, these statistics are not available.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
WAN1 TrafficMeter
WAN2 TrafficMeter
WAN3 TrafficMeter
WAN4 TrafficMeter
Traffic by Protocol
Help
Apply
Reset

Enable Traffic Meter

Do you want to enable Traffic Metering on WAN1?

● Yes

○ No

● No Limit

○ Download only

○ Both Directions

Monthly Limit: 0 [MB] [max. 256000 MB (~250 GB)]

□ Increase this month limit by:

0 [MB] [max. 256000 MB (~250 GB)]

This month limit: 0 [MB]

Traffic Counter

○ Restart Traffic Counter Now

● Restart Traffic Counter at Specific Time

12 :00 AM on the 1st day of Month.

□ Send e-mail report before restarting counter

When Limit is reached

● Block All Traffic

○ Block All Traffic Except E-Mail

□ Send e-mail alert

Internet Traffic Statistics

Start Date / Time:

Outgoing Traffic Volume: [MB]

Incoming Traffic Volume: [MB]

Total Traffic Volume: [MB]

Average per day: [MB]

% of Standard Limit:

% of this Month's Limit:

Figure 159.

2. Enter the settings for the WAN1 port as explained in the following table:

Table 65. WAN Traffic Meter screen settings

Setting	Description
Enable Traffic Meter	
Do you want to enable Traffic Metering on WAN1?	Select one of the following radio buttons to configure traffic metering: • **Yes**. Traffic metering is enabled, and the traffic meter records the volume of Internet traffic passing through the WAN1 interface. Complete the fields that are shown on the right side of the screen (see explanations later in this table). • **No**. Traffic metering is disabled. This is the default setting.

Table 65. WAN Traffic Meter screen settings (continued)

Setting	Description	
Do you want to enable Traffic Metering on WAN1? (continued)	Select one of the following radio buttons to specify if or how the VPN firewall applies restrictions when the traffic limit is reached: • **No Limit**. No restrictions are applied when the traffic limit is reached. • **Download only**. Restrictions are applied to incoming traffic when the traffic limit is reached. Complete the Monthly Limit field. • **Both Directions**. Restrictions are applied to both incoming and outgoing traffic when the traffic limit is reached. Complete the Monthly Limit field.	
	Monthly Limit	Enter the monthly traffic volume limit in MB. The default setting is 0 MB.
	Increase this month limit by	Select this check box to temporarily increase a previously specified monthly traffic volume limit, and enter the additional allowed volume in MB. The default setting is 0 MB. **Note:** When you click Apply to save these settings, this field is reset to 0 MB so that the increase is applied only once.
	This month limit	This is a nonconfigurable field that displays the total monthly traffic volume limit that is applicable to this month. This total is the sum of the monthly traffic volume and the increased traffic volume.
Traffic Counter		
Restart Traffic Counter	Select one of the following radio buttons to specify when the traffic counter restarts: • **Restart Traffic Counter Now**. Select this option and click **Apply** at the bottom of the screen to restart the traffic counter immediately. • **Restart Traffic Counter at a Specific Time**. Restart the traffic counter at a specific time and day of the month. Fill in the time fields and select AM or PM and the day of the month from the drop-down lists.	
Send e-mail report before restarting counter	An email report is sent immediately before the counter restarts. Ensure that emailing of logs is enabled on the Email and Syslog screen (see *Activate Notification of Events, Alerts, and Syslogs* on page 269).	
When Limit is reached		
Block Traffic	Select one of the following radio buttons to specify what action the VPN firewall performs when the traffic limit has been reached: • **Block All Traffic**. All incoming and outgoing Internet and email traffic is blocked. • **Block All Traffic Except E-Mail**. All incoming and outgoing Internet traffic is blocked, but incoming and outgoing email traffic is still allowed.	
Send e-mail alert	An email alert is sent when traffic is blocked. Ensure that emailing of logs is enabled on the Email and Syslog screen (see *Activate Notification of Events, Alerts, and Syslogs* on page 269).	

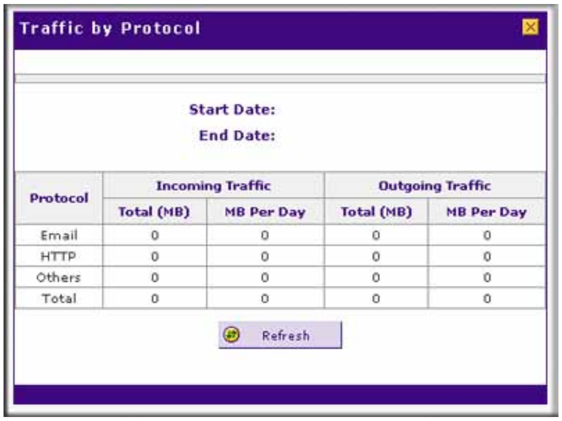
3. Click **Apply** to save your settings.
4. If you want to enable the traffic meter for another WAN interface, select the appropriate WAN Traffic Meter tab for that interface, and repeat *step 2* and *step 3* for that WAN interface.

The contents of the WAN2 Traffic Meter, WAN3 Traffic Meter, and WAN4 Traffic Meter screens are identical to the WAN1 TrafficMeter screen with the exception of WAN interface number.

➢ **To display a report of the Internet traffic by type for the WAN1 interface:**

Click the **Traffic by Protocol** option arrow in the upper right of the WAN1 Traffic Meter screen. (Each WAN TrafficMeter screen has a Traffic by Protocol option arrow that enables you to display the Internet traffic by type for that WAN interface.)

The Traffic by Protocol screen appears in a popup window:



Start Date:

End Date:

Protocol	Incoming Traffic		Outgoing Traffic	
	Total (MB)	MB Per Day	Total (MB)	MB Per Day
Email	0	0	0	0
HTTP	0	0	0	0
Others	0	0	0	0
Total	0	0	0	0

Figure 160.

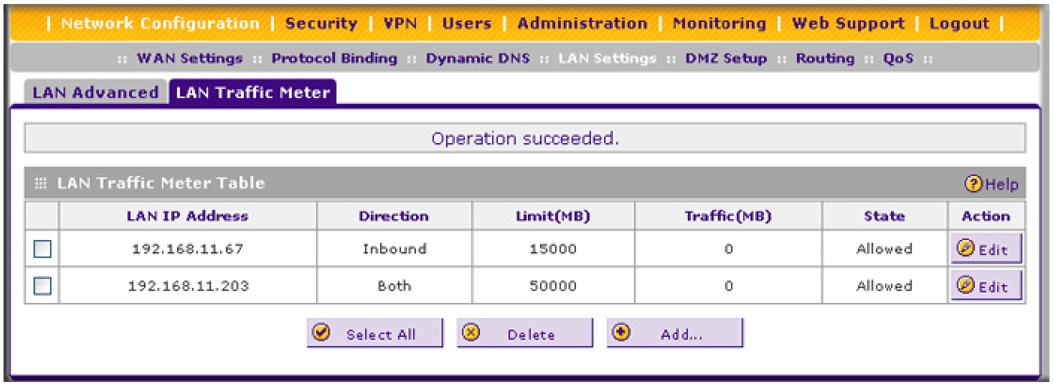
The incoming and outgoing volume of traffic for each protocol and the total volume of traffic are displayed. Traffic counters are updated in MBs; the counter starts only when traffic passed is at least 1 MB. In addition, the popup screen displays the traffic meter’s start and end dates.

Enable the LAN Traffic Meter

If your ISP charges by traffic volume over a period of time and you need to charge the costs to individual accounts, or if you want to study the traffic volume that is requested or sent over a LAN IP address over a period of time, you can activate the traffic meter for individual LAN IP addresses.

➢ **To monitor traffic for LAN IP addresses:**

1. Select **Network Configuration > LAN Settings**. The LAN submenu tabs display, with the LAN Setup screen in view (see *Figure 30* on page 59).
2. Select the **Advanced** option arrow in the upper right of the LAN Setup screen. The LAN Advanced screen displays.
3. Select the LAN Traffic Meter tab. The LAN Traffic Meter screen displays. (The following figure shows some examples in the LAN Traffic Meter table.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
LAN Advanced
LAN Traffic Meter
LAN Traffic Meter Table
Help
Select All
Delete
Add...

Operation succeeded.

	LAN IP Address	Direction	Limit(MB)	Traffic(MB)	State	Action
□	192.168.11.67	Inbound	15000	0	Allowed	Edit
□	192.168.11.203	Both	50000	0	Allowed	Edit

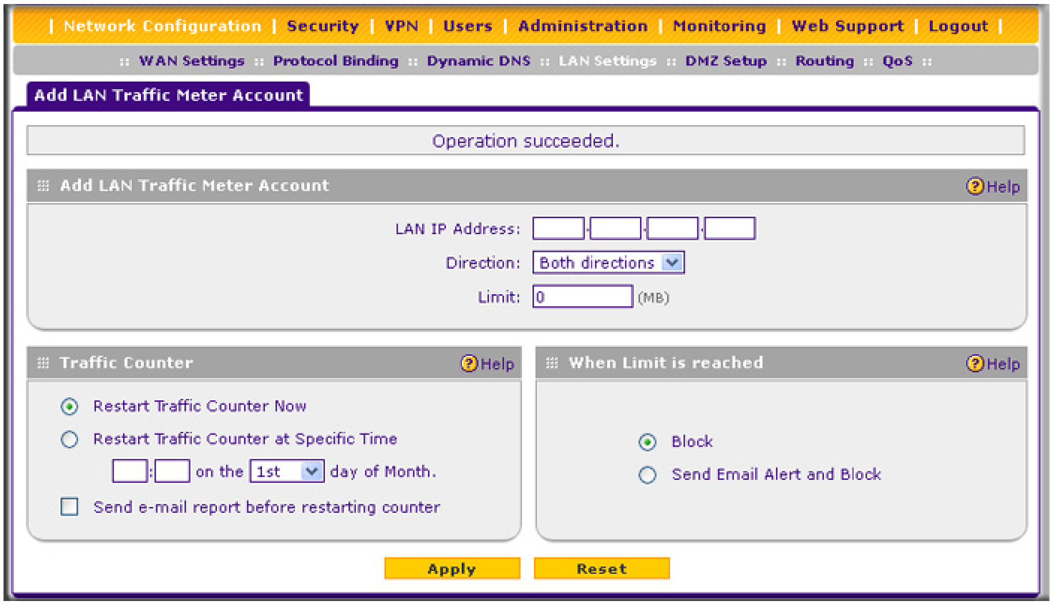
Figure 161.

The LAN Traffic Meter table show the following columns, all of which are explained in detail in the following table:

- **LAN IP Address**. The LAN IP address that is subject to the traffic meter.
- **Direction**. The direction for which traffic is measured.
- **Limit(MB)**. The traffic limit in MB.
- **Traffic(MB)**. The traffic usage in MB.
- **State**. The state that indicates whether traffic to and from the IP address is allowed or blocked.
- **Action**. The Edit table button provides access to the Edit LAN Traffic Meter screen for the corresponding IP address.

➢ To add a LAN IP address account to the traffic meter:

4. On the LAN Traffic Meter screen, click the **Add** table button. The Add LAN Traffic Meter screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
Add LAN Traffic Meter Account
Add LAN Traffic Meter Account
Help
Traffic Counter
Help
When Limit is reached
Help
Apply
Reset

Operation succeeded.

LAN IP Address: [ ].[ ].[ ].[ ]
Direction: Both directions
Limit: 0 (MB)

● Restart Traffic Counter Now
○ Restart Traffic Counter at Specific Time
[ ]:[ ] on the 1st day of Month.
□ Send e-mail report before restarting counter

● Block
○ Send Email Alert and Block

Figure 162.

5. Enter the settings as explained in the following table:

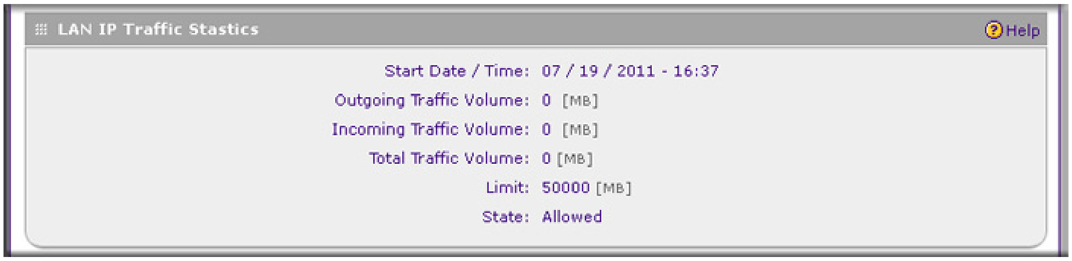
Table 66. Add LAN Traffic Meter Account screen settings

Setting	Description
Add LAN Traffic Meter Account	
LAN IP Address	The LAN IP address for the account.
Direction	From the Direction drop-down list, select the direction in which traffic is measured: • **Inbound traffic**. Restrictions are applied to incoming traffic when the traffic limit is reached. • **Both directions**. Restrictions are applied to both incoming and outgoing traffic when the traffic limit is reached.
Limit	Enter the monthly traffic volume limit in MB. The default setting is 0 MB.
Traffic Counter	
Restart Traffic Counter	Select one of the following radio buttons to specify when the traffic counter restarts: • **Restart Traffic Counter Now**. Select this option and click **Apply** at the bottom of the screen to restart the traffic counter immediately. • **Restart Traffic Counter at a Specific Time**. Restart the traffic counter at a specific time and day of the month. Fill in the time fields and select the day of the month from the drop-down list.
Send e-mail report before restarting counter	An email report is sent immediately before the counter restarts. Ensure that emailing of logs is enabled on the Email and Syslog screen (see *Activate Notification of Events, Alerts, and Syslogs* on page 269).
When Limit is reached	
Block Traffic	Select one of the following radio buttons to specify what action the VPN firewall performs when the traffic limit has been reached: • **Block**. All incoming and outgoing Internet and email traffic is blocked. • **Send Email Alert and Block**. An email alert is sent when all incoming and outgoing Internet and email traffic is blocked. Ensure that emailing of logs is enabled on the Email and Syslog screen (see *Activate Notification of Events, Alerts, and Syslogs* on page 269).

6. Click **Apply** to save your settings. The new account is added to the LAN Traffic Meter table on the LAN Traffic Meter screen.

➢ To view the LAN IP traffic meter statistics:

In the LAN Traffic Meter table, click the **Edit** table button to the right of the account for which you want to view the statistics. The Edit LAN Traffic Meter Account screen displays. This screen shows the same fields as the Add LAN Traffic Meter Account screen (see the previous figure) together with the statistics at the bottom of the screen:



Start Date / Time: 07 / 19 / 2011 - 16:37
Outgoing Traffic Volume: 0 [MB]
Incoming Traffic Volume: 0 [MB]
Total Traffic Volume: 0 [MB]
Limit: 50000 [MB]
State: Allowed

Figure 163.

➤ To edit a LAN traffic meter account:

1. In the LAN Traffic Meter table, click the **Edit** table button to the right of the account that you want to edit. The Edit LAN Traffic Meter Account screen displays. This screen shows the same fields as the Add LAN Traffic Meter Account screen (see *Figure 162* on page 267).
2. Modify the settings as explained in the previous table.
3. Click **Apply** to save your settings.

➤ To delete a LAN traffic meter account:

1. Select the check box to the left of the account that you want to delete, or click the **Select All** table button to select all accounts.
2. Click the **Delete** table button.

Activate Notification of Events, Alerts, and Syslogs

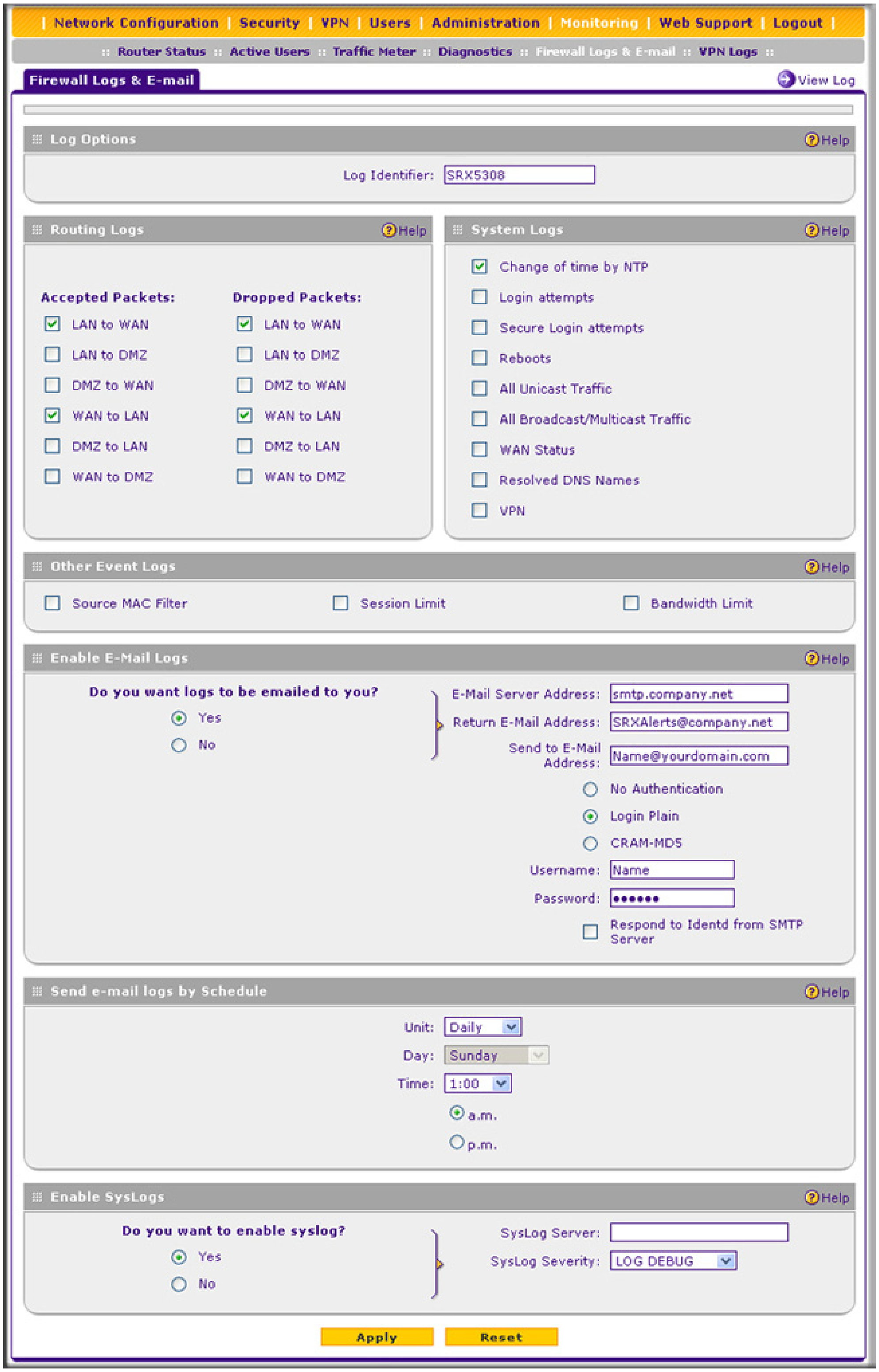
You can configure the VPN firewall to log and then email denial of access, general attacks, and other information to a specified email address. For example, the VPN firewall can log security-related events such as accepted and dropped packets on different segments of your LAN, denied incoming and outgoing service requests, hacker probes and login attempts, and other general information based on the settings that you specify on the Firewall Logs & E-mail screen. Selecting all events will increase the size of the log, so it is good practice to select only those events that are required.

For you to receive the logs in an email message, the VPN firewall's email notification server needs to be configured and email notification needs to be enabled. You need to configure the necessary information for sending email, such as the administrator's email address, the email server, user name, and password.

You can also view the logs on the View Log screen or send them to a syslog server.

➤ To configure and activate logs:

1. Select **Monitoring > Firewall Logs & E-mail**. The Firewall Logs & E-mail screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
View Log
Help
Apply
Reset

Firewall Logs & E-mail

Log Options

Log Identifier: SRX5308

Routing Logs

Accepted Packets:	Dropped Packets:
☑ LAN to WAN	☑ LAN to WAN
□ LAN to DMZ	□ LAN to DMZ
□ DMZ to WAN	□ DMZ to WAN
☑ WAN to LAN	☑ WAN to LAN
□ DMZ to LAN	□ DMZ to LAN
□ WAN to DMZ	□ WAN to DMZ

System Logs

☑ Change of time by NTP
□ Login attempts
□ Secure Login attempts
□ Reboots
□ All Unicast Traffic
□ All Broadcast/Multicast Traffic
□ WAN Status
□ Resolved DNS Names
□ VPN

Other Event Logs

□ Source MAC Filter □ Session Limit □ Bandwidth Limit

Enable E-Mail Logs

Do you want logs to be emailed to you?
● Yes
○ No

E-Mail Server Address: smtp.company.net
Return E-Mail Address: SRXAlerts@company.net
Send to E-Mail Address: Name@yourdomain.com
○ No Authentication
● Login Plain
○ CRAM-MD5
Username: Name
Password: ●●●●●●
□ Respond to Identd from SMTP Server

Send e-mail logs by Schedule

Unit: Daily
Day: Sunday
Time: 1:00
● a.m.
○ p.m.

Enable SysLogs

Do you want to enable syslog?
● Yes
○ No

SysLog Server:
SysLog Severity: LOG DEBUG

Figure 164.

2. Enter the settings as explained in the following table:

Table 67. Firewall Logs & E-mail screen settings

Setting	Description
Log Options	
Log Identifier	Enter the name of the log in the Log Identifier field. The Log Identifier is a mandatory field used to identify which device sent the log messages. The identifier is appended to the log messages. The default identifier is SRX5308.
Routing Logs	
From the Accepted Packets and Dropped Packets columns, select check boxes to specify which traffic is logged: • **LAN to WAN** • **LAN to DMZ** • **DMZ to WAN** • **WAN to LAN** • **DMZ to LAN** • **WAN to DMZ**	
System Logs	
Select the check boxes to specify which system events are logged: • **Change of Time by NTP**. Logs a message when the system time changes after a request from an NTP server. • **Login Attempts**. Logs a message when a login is attempted. Both successful and failed login attempts are logged. • **Secure Login Attempts**. Logs a message when a secure login is attempted. Both successful and failed secure login attempts are logged. • **Reboots**. Logs a message when the VPN firewall has been rebooted through the web management interface. (No message is logged when the reset button has been pushed to reboot the VPN firewall.) • **All Unicast Traffic**. All incoming unicast packets are logged. • **All Broadcast/Multicast Traffic**. All incoming broadcast and multicast packets are logged. • **WAN Status**. WAN link status–related events are logged. • **Resolved DNS Names**. All resolved DNS names are logged. • **VPN**. All VPN events are logged.	
Other Event Logs	
Source MAC Filter	Select this check box to log packets from MAC addresses that match the source MAC address filter settings (see *Enable Source MAC Filtering* on page 126).
Session Limit	Select this check box to log packets that are dropped because the session limit has been exceeded (see *Set Session Limits* on page 109).
Bandwidth Limit	Select this check box to log packets that are dropped because the bandwidth limit has been exceeded (see *Create Bandwidth Profiles* on page 118).

Table 67. Firewall Logs & E-mail screen settings (continued)

Setting	Description	
Enable E-Mail Logs		
Do you want logs to be emailed to you?	Select the **Yes** radio button to enable the VPN firewall to send logs to an email address. Complete the fields that are shown on the right side of the screen (see explanations later in this table). Select the **No** radio button to disable the VPN firewall to send logs to an email address, which is the default setting.	
	E-Mail Server Address	The IP address or Internet name of your ISP's outgoing email SMTP server. **Note:** If you leave this field blank, the VPN firewall cannot send email logs and alerts.
	Return E-Mail Address	A descriptive name of the sender for email identification purposes. For example, enter SRXAlerts@company.com.
	Send to E-Mail Address:	The email address to which the notifications are sent. Typically, this is the email address of an administrator.
	Select one of the following radio buttons to specify SMTP server authentication: • **No Authentication**. The SMTP server does not require authentication. • **Login Plain**. The SMTP server requires authentication with regular login. Specify the user name and password to be used for authentication. • **CRAM-MD5**. The SMTP server requires authentication with CRAM-MD5 login. Specify the user name and password to be used for authentication.	
	User name	The user name for SMTP server authentication.
	Password	The password for SMTP server authentication.
	Respond to Identd from SMTP Server	Select the **Respond to Identd from SMTP Server** check box to respond to Ident protocol messages. The Ident protocol is a weak scheme to verify the sender of an email. (A common daemon program for providing the Ident service is Identd).
Send e-mail logs by Schedule		
Unit	Enter a schedule for sending the logs. From the Unit drop-down list, select one of the following: • **Never**. No logs are sent. • **Hourly**. The logs are sent every hour. • **Daily**. The logs are sent daily. Specify the time. • **Weekly**. The logs are sent weekly. Specify the day and time.	
	Day	From the Day drop-down list, select the day on which the logs are sent.
	Time	From the Time drop-down list select the hour on which the logs are sent, and then select either the **a.m.** or **p.m.** radio button.

Table 67. Firewall Logs & E-mail screen settings (continued)

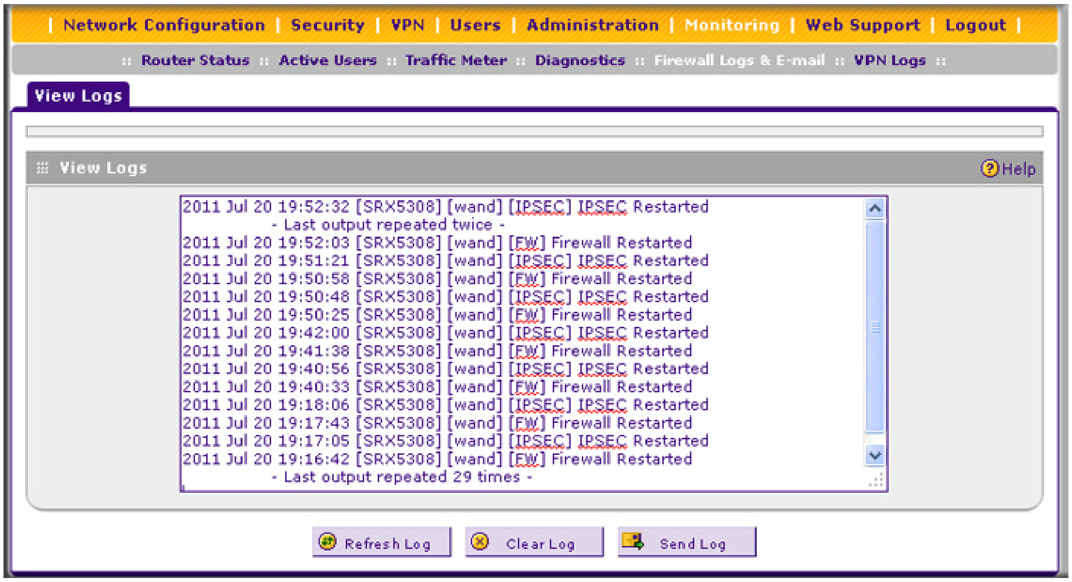
Setting	Description	
Enable SysLogs		
Enable	Select one of the following radio buttons to configure the syslog server: **Yes**. The VPN firewall sends a log file to a syslog server. Complete the SysLog Server and SysLog Severity fields that are shown on the right side of the screen (see explanations later in this table). • **No**. The VPN firewall does not send a log file to a syslog server, which is the default setting.	
	SysLog Server	The IP address or name of the syslog server.
	SysLog Severity	All the logs with a severity that is equal to and above the severity that you specify are logged on the specified syslog server. For example, if you select LOG_CRITICAL as the severity, then the logs with the severities LOG_CRITICAL, LOG_ALERT, and LOG_EMERG are logged. From the SysLog Severity drop-down list, select one of the following syslog severities: • **LOG EMERG**. The VPN firewall is unusable. • **LOG ALERT**. An action needs to be taken immediately. • **LOG CRITICAL**. There are critical conditions. • **LOG ERROR**. There are error conditions. • **LOG WARNING**. There are warning conditions. • **LOG NOTICE**. There are normal but significant conditions. • **LOG INFO**. Informational messages. • **LOG DEBUG**. Debug-level messages.

3. Click **Apply** to save your settings.

Note: Enabling logs might generate a significant volume of log messages. NETGEAR recommends that you enable firewall logs for debugging purposes only.

➢ To view the routing logs, system logs, and other event logs onscreen:

1. Select **Monitoring > Firewall Logs & E-mail**. The Firewall Logs & E-mail screen displays.
2. Click the **View Log** option arrow in the upper right of the Firewall Logs & E-mai screen. The View Log screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
View Logs
View Logs
Help
Refresh Log
Clear Log
Send Log

```
2011 Jul 20 19:52:32 [SRX5308] [wand] [IPSEC] IPSEC Restarted
              - Last output repeated twice -
2011 Jul 20 19:52:03 [SRX5308] [wand] [FW] Firewall Restarted
2011 Jul 20 19:51:21 [SRX5308] [wand] [IPSEC] IPSEC Restarted
2011 Jul 20 19:50:58 [SRX5308] [wand] [FW] Firewall Restarted
2011 Jul 20 19:50:48 [SRX5308] [wand] [IPSEC] IPSEC Restarted
2011 Jul 20 19:50:25 [SRX5308] [wand] [FW] Firewall Restarted
2011 Jul 20 19:42:00 [SRX5308] [wand] [IPSEC] IPSEC Restarted
2011 Jul 20 19:41:38 [SRX5308] [wand] [FW] Firewall Restarted
2011 Jul 20 19:40:56 [SRX5308] [wand] [IPSEC] IPSEC Restarted
2011 Jul 20 19:40:33 [SRX5308] [wand] [FW] Firewall Restarted
2011 Jul 20 19:18:06 [SRX5308] [wand] [IPSEC] IPSEC Restarted
2011 Jul 20 19:17:43 [SRX5308] [wand] [FW] Firewall Restarted
2011 Jul 20 19:17:05 [SRX5308] [wand] [IPSEC] IPSEC Restarted
2011 Jul 20 19:16:42 [SRX5308] [wand] [FW] Firewall Restarted
              - Last output repeated 29 times -
```

Figure 165.

You can refresh the logs, clear the logs, or send the logs to an email address.

View Status and Log Screens

The VPN firewall provides real-time information in a variety of status screens that are described in the following sections:

- *View the System (Router) Status and Statistics*
- *View the VLAN Status*
- *View and Disconnect Active Users*
- *View the VPN Tunnel Connection Status*
- *View the VPN Logs*
- *View the Port Triggering Status*
- *View the WAN Port Connection Status*
- *View the Attached Devices and DHCP Log*

View the System (Router) Status and Statistics

The Router Status screen, Detailed Status screen, and Router Statistics screen provide real-time information about the following important components of the VPN firewall:

- Firmware versions that are loaded on the VPN firewall
- WAN and LAN port information
- Interface statistics

View the Router Status Screen

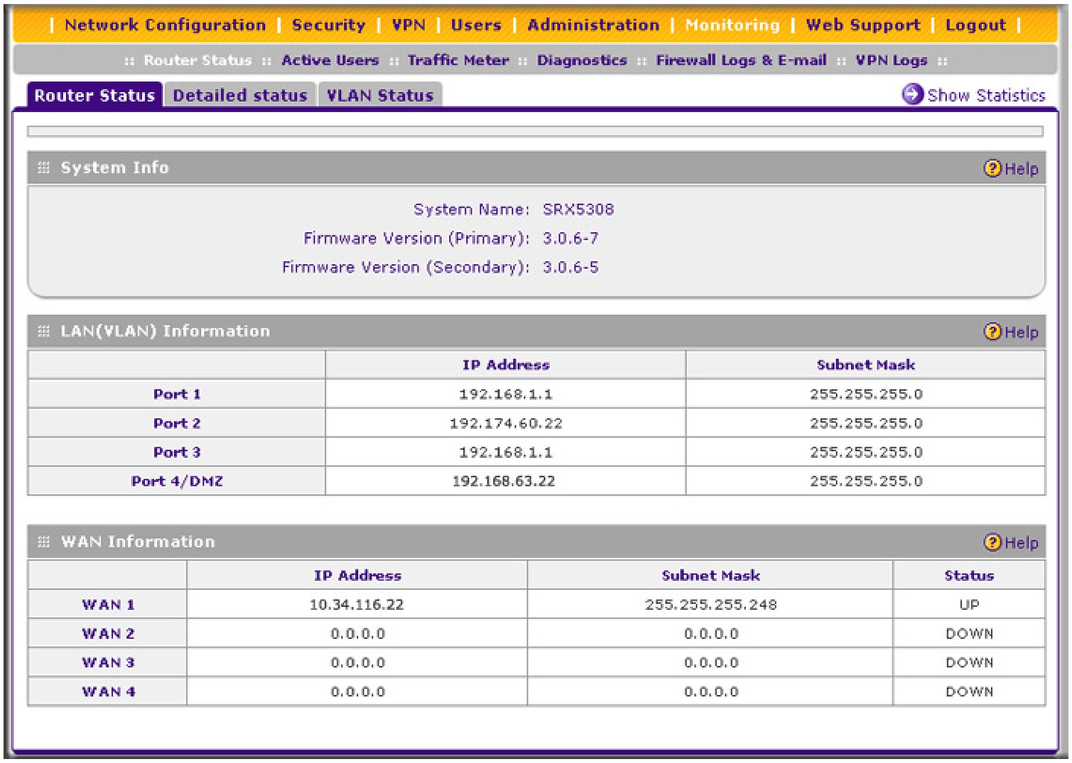
➢ **To view the Router Status screen:**

Select **Monitoring > Router Status**. The Status tabs display, with the Router Status screen in view (see the following figure).

The following table explains the fields of the Router Status screen:

Table 68. Router Status screen information

Item	Description
System Info	
System Name	The NETGEAR product name.
Firmware Version (Primary)	The current software version that the VPN firewall is using.
Firmware Version (Secondary)	The secondary software version. This version is for display only. (In the current release, you cannot configure this version.)
LAN (VLAN) Information	
For each of the four LAN ports, the screen shows the IP address and subnet mask. For more detailed information, see the following table.	
WAN Information	
For each of the four WAN ports, the screen shows the IP address, subnet mask, and status of the port (UP or DOWN). For more detailed information, see the following table.	


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Router Status
Detailed status
VLAN Status
Show Statistics
Help
Help
Help

System Info

System Name: SRX5308

Firmware Version (Primary): 3.0.6-7

Firmware Version (Secondary): 3.0.6-5

LAN(VLAN) Information

	IP Address	Subnet Mask
Port 1	192.168.1.1	255.255.255.0
Port 2	192.174.60.22	255.255.255.0
Port 3	192.168.1.1	255.255.255.0
Port 4/DMZ	192.168.63.22	255.255.255.0

WAN Information

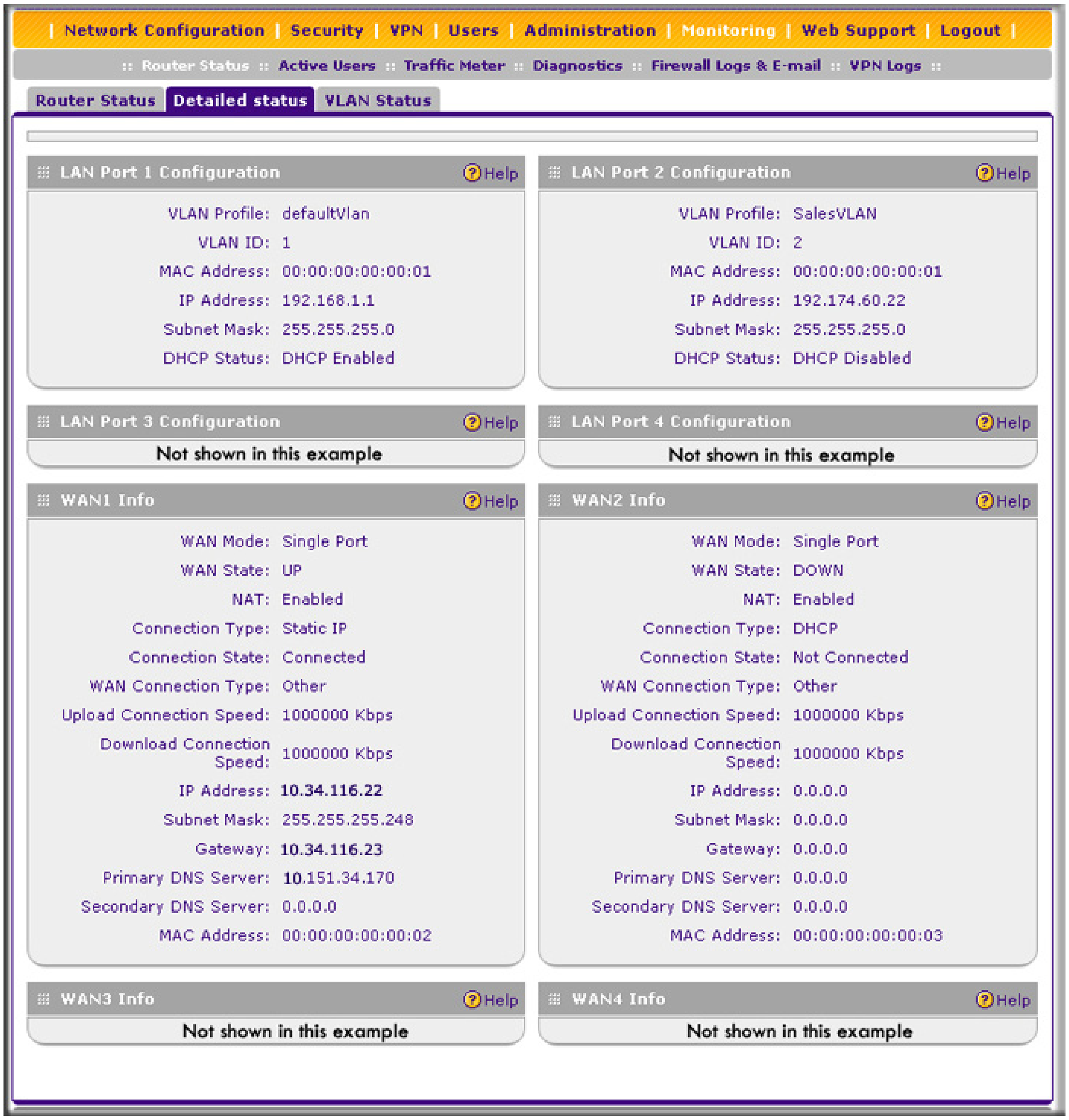
	IP Address	Subnet Mask	Status
WAN 1	10.34.116.22	255.255.255.248	UP
WAN 2	0.0.0.0	0.0.0.0	DOWN
WAN 3	0.0.0.0	0.0.0.0	DOWN
WAN 4	0.0.0.0	0.0.0.0	DOWN

Figure 166.

View the Detailed Status Screen

➢ **To view the Detailed Status screen:**

1. Select **Monitoring > Router Status > Detailed Status**. The Detailed Status screen displays. (Because of the large size of the screen and to avoid duplication of information, the following figure shows parts of the screen.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Router Status
Detailed status
VLAN Status
Help

LAN Port 1 Configuration

VLAN Profile: defaultVlan
VLAN ID: 1
MAC Address: 00:00:00:00:00:01
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHCP Status: DHCP Enabled

LAN Port 2 Configuration

VLAN Profile: SalesVLAN
VLAN ID: 2
MAC Address: 00:00:00:00:00:01
IP Address: 192.174.60.22
Subnet Mask: 255.255.255.0
DHCP Status: DHCP Disabled

LAN Port 3 Configuration

Not shown in this example

LAN Port 4 Configuration

Not shown in this example

WAN1 Info

WAN Mode: Single Port
WAN State: UP
NAT: Enabled
Connection Type: Static IP
Connection State: Connected
WAN Connection Type: Other
Upload Connection Speed: 1000000 Kbps
Download Connection Speed: 1000000 Kbps
IP Address: 10.34.116.22
Subnet Mask: 255.255.255.248
Gateway: 10.34.116.23
Primary DNS Server: 10.151.34.170
Secondary DNS Server: 0.0.0.0
MAC Address: 00:00:00:00:00:02

WAN2 Info

WAN Mode: Single Port
WAN State: DOWN
NAT: Enabled
Connection Type: DHCP
Connection State: Not Connected
WAN Connection Type: Other
Upload Connection Speed: 1000000 Kbps
Download Connection Speed: 1000000 Kbps
IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Gateway: 0.0.0.0
Primary DNS Server: 0.0.0.0
Secondary DNS Server: 0.0.0.0
MAC Address: 00:00:00:00:00:03

WAN3 Info

Not shown in this example

WAN4 Info

Not shown in this example

Figure 167.

The following table explains the fields of the Detailed Status screen:

Table 69. Detailed Status screen information

Item	Description
LAN Port Configuration The following fields are shown for each of the four LAN port.	
VLAN Profile	The name of the VLAN profile that you assigned to this port on the LAN Setup screen (see *Assign and Manage VLAN Profiles* on page 57). If the VLAN is not enabled on this port, the default profile (with VLAN ID 1) is assigned automatically.

Table 69. Detailed Status screen information (continued)

Item	Description
VLAN ID	The VLAN ID that you assigned to this port on the Add VLAN Profile screen (see *Configure a VLAN Profile* on page 59). If the default VLAN profile is used, the VLAN ID is 1, which means that all tagged and untagged traffic can pass on this port.
MAC Address	The MAC address of this port. All LAN ports share the same MAC address (00:00:00:00:00:01). However, if LAN port 4 is enabled as the DMZ port, its MAC address is changed to 00:00:00:00:00:06. For information about configuring the DMZ port, see *Configure and Enable the DMZ Port* on page 72.
IP Address	The IP address for this port. If the VLAN is not enabled on this port, the IP address is the default LAN IP address (192.168.1.1). For information about configuring VLAN profiles, see *Configure a VLAN Profile* on page 59.
Subnet Mask	The subnet mask for this port. If the VLAN is not enabled on this port, the subnet mask is the default LAN IP subnet mask (255.255.255.0). For information about configuring VLAN profiles, see *Configure a VLAN Profile* on page 59.
DHCP Status	The status can be either DHCP Enabled or DHCP Disabled. For information about enabling DHCP for this port, see *Configure a VLAN Profile* on page 59.
WAN Info The following fields are shown for each of the four WAN port.	
WAN Mode	The WAN mode can be Single Port, Load Balancing, or Auto Rollover. For information about configuring the WAN mode, see *Configure the WAN Mode* on page 32.
WAN State	The WAN state can be either UP or DOWN, depending on whether the port is connected to the Internet and whether the port is enabled. For information about connecting WAN ports, see *Configure the Internet Connections* on page 24.
NAT	The NAT state can be either Enabled or Disabled, depending on whether NAT is enabled (see *Configure Network Address Translation* on page 33) or classical routing is enabled (see *Configure Classical Routing* on page 33).
Connection Type	The connection type can be Static IP, DHCP, PPPoE, or PPTP, depending on whether the WAN address is obtained dynamically through a DHCP server or assigned statically by you. For information about connection types, see *Configure the Internet Connections* on page 24.
Connection State	The connection state can be either Connected or Not Connected, depending on whether the WAN port is physically connected to a modem or router. For information about connecting a WAN port, see the *ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308 Installation Guide*.
WAN Connection Type	The detected type of Internet connection that is used on this port. The WAN connection type can be DSL, ADSL, CableModem, T1, or T3.
Upload Connection Speed	The maximum upload speed that is provided by your ISP.
Download Connection Speed	The maximum download speed that is provided by your ISP.

Table 69. Detailed Status screen information (continued)

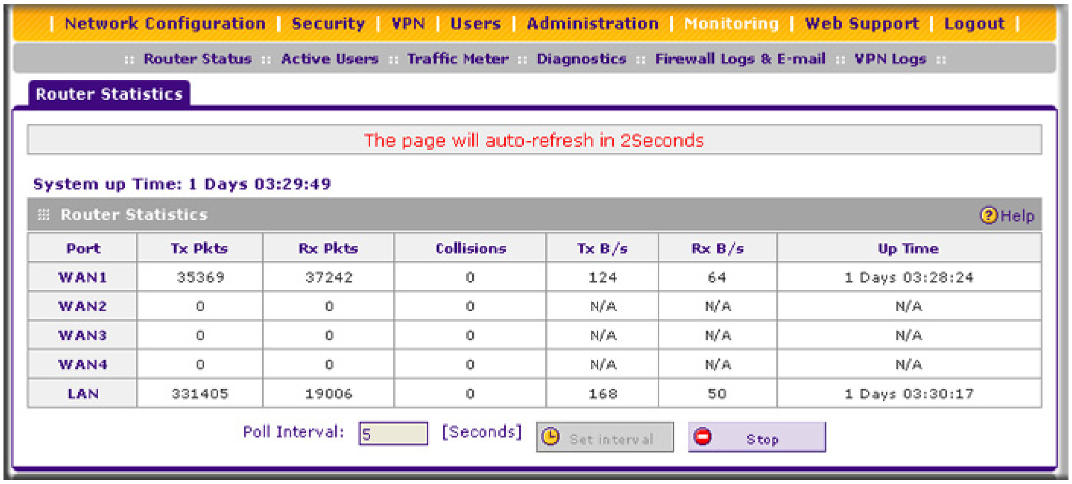
Item	Description	
IP Address	The IP address of the WAN port.	These settings are either obtained dynamically from your ISP or specified by you on the WAN ISP Settings screen for this port (see *Manually Configure the Internet Connection* on page 28).
Subnet Mask	The subnet mask of the WAN port.	
Gateway	The IP address of the gateway.	
Primary DNS Server	The IP address of the primary DNS server.	
Secondary DNS Server	The IP address of the secondary DNS server.	
MAC Address	The default MAC address for this port (for more information, see the note following this table) or the MAC address that you have specified on the WAN Advanced Options screen for this port. For information about configuring the MAC address, see *Configure Advanced WAN Options* on page 51.	

Note: The default MAC addresses for the LAN and WAN ports are
00:00:00:00:00:01, shared by the LAN1, LAN2, LAN3, and LAN4 ports.
00:00:00:00:00:02, unique for WAN1 port.
00:00:00:00:00:03, unique for WAN2 port.
00:00:00:00:00:04, unique for WAN3 port.
00:00:00:00:00:05, unique for WAN4 port.
00:00:00:00:00:06, unique for DMZ port (LAN4 port), if enabled.

View the Router Statistics Screen

➤ **To view the Router Statistics screen:**

1. Select **Monitoring > Router Status**. The Status tabs display, with the Router Status screen in view (see *Figure 166* on page 276).
2. Click the **Show Statistics** option arrow in the upper right of the Router Status screen. The Router Statistics screen displays.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Router Statistics
Router Statistics
Help
Set interval
Stop

The page will auto-refresh in 2Seconds

System up Time: 1 Days 03:29:49

Port	Tx Pkts	Rx Pkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN1	35369	37242	0	124	64	1 Days 03:28:24
WAN2	0	0	0	N/A	N/A	N/A
WAN3	0	0	0	N/A	N/A	N/A
WAN4	0	0	0	N/A	N/A	N/A
LAN	331405	19006	0	168	50	1 Days 03:30:17

Poll Interval: 5 [Seconds]

The following table explains the fields of the Router Statistics screen:

Table 70. Router Statistics screen information

Item	Description
System up Time: the period since the last time that the VPN firewall was started up.	
Router Statistics	
For each of the four WAN interfaces and for all LAN interfaces combined, the following statistics are displayed:	
Tx Pkts	The number of transmitted packets on the port in bytes.
Rx Pxts	The number of received packets on the port in bytes.
Collisions	The number of signal collisions that have occurred on the port. A collision occurs when the port attempts to send data at the same time as a port on the other router or computer that is connected to this port.
Tx B/s	The number of transmitted bytes per second on the port.
Rx B/s	The number of received bytes per second on the port.
Up TIme	The period that the port has been active since it was restarted.

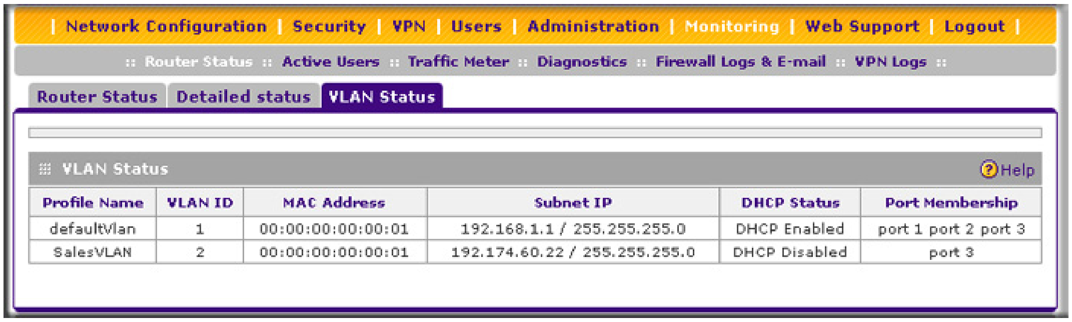
To change the poll interval period, enter a new value in the Poll Interval field, and then click **Set interval**. To stop polling, click **Stop**.

View the VLAN Status

The VLAN Status screen displays information about the VLANs (both enabled and disabled) that are configured on the VPN firewall. For information about configuring VLAN profiles, see *Configure a VLAN Profile* on page 59. For information about enabling and disabling VLAN profiles, see *Assign and Manage VLAN Profiles* on page 57.

To view the VLAN Status screen:

Select **Monitoring > Router Status > VLAN Status**. The VLAN Status screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Router Status
Detailed status
VLAN Status
VLAN Status
Help

Profile Name	VLAN ID	MAC Address	Subnet IP	DHCP Status	Port Membership
defaultVlan	1	00:00:00:00:00:01	192.168.1.1 / 255.255.255.0	DHCP Enabled	port 1 port 2 port 3
SalesVLAN	2	00:00:00:00:00:01	192.174.60.22 / 255.255.255.0	DHCP Disabled	port 3

Figure 168.

The following table explains the fields of the VLAN Status screen:

Table 71. VLAN Status screen information

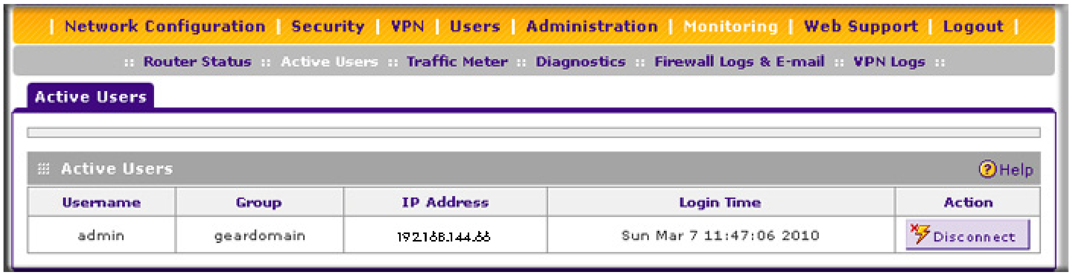
Item	Description
Profile Name	The unique name for the VLAN that you have assigned on the Add VLAN Profile screen (see *Configure a VLAN Profile* on page 59).
VLAN ID	The identifier for the VLAN that you have assigned on the Add VLAN Profile screen (see *Configure a VLAN Profile* on page 59).
MAC Address	VLANs can have the same MAC address as the associated LAN port or can be assigned a unique MAC address, depending on the selection that you have made on the LAN Advanced screen (see *Configure VLAN MAC Addresses and LAN Advanced Settings* on page 64). If a VLAN is configured but disabled, the MAC address displays as 00:00:00:00:00:00.
Subnet IP	The IP address and subnet mask that you have assigned on the Add VLAN Profile screen (see *Configure a VLAN Profile* on page 59).
DHCP Status	The DHCP status for the VLAN, which can be either DHCP Enabled or DHCP Disabled, depending on the DHCP configuration that you have specified on the Add VLAN Profile screen (see *Configure a VLAN Profile* on page 59).
Port Membership	The ports that you have associated with the VLAN on the Add VLAN Profile screen (see *Configure a VLAN Profile* on page 59).

View and Disconnect Active Users

The Active Users screen displays a list of administrators, IPSec VPN, and SSL VPN users that are currently logged in to the VPN firewall.

To display the list of active VPN users:

Select **Monitoring > Active Users**. The Active Users screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Active Users
Help
Disconnect

Active Users

Username	Group	IP Address	Login Time	Action
admin	geardomain	192.168.144.66	Sun Mar 7 11:47:06 2010	Disconnect

Figure 169.

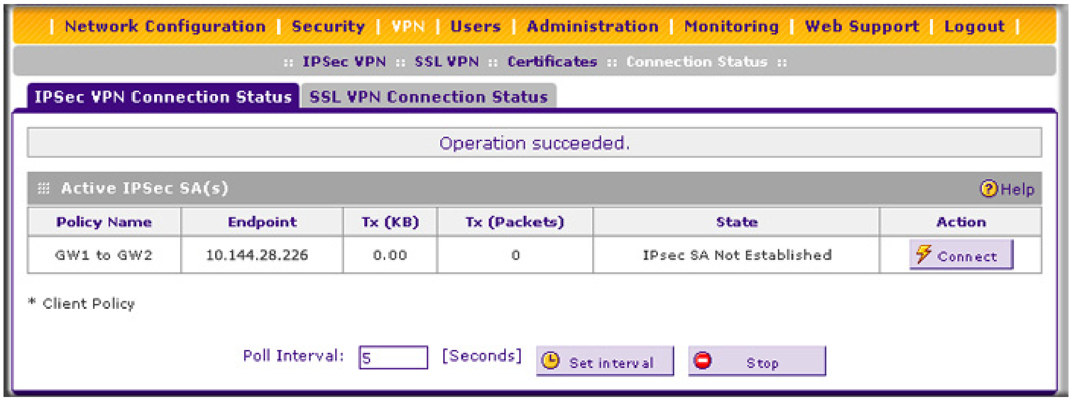
The active user's user name, group, and IP address are listed in the table with a timestamp indicating the time and date that the user logged in.

To disconnect an active user, click the **Disconnect** table button to the right of the user's table entry.

View the VPN Tunnel Connection Status

➤ To view the status of current IPSec VPN tunnels:

Select **VPN > Connection Status**. The VPN Connection Status submenu tabs display, with the IPSec VPN Connection Status screen in view. (The following figure shows an IPSec SA as an example.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: Certificates :: Connection Status ::
IPSec VPN Connection Status
SSL VPN Connection Status
Help
Connect
Set interval
Stop

Operation succeeded.

Active IPSec SA(s)

Policy Name	Endpoint	Tx (KB)	Tx (Packets)	State	Action
GW1 to GW2	10.144.28.226	0.00	0	IPsec SA Not Established	Connect

* Client Policy

Poll Interval: 5 [Seconds]

Figure 170.

The Active IPSec SAs table lists each active connection with the information that is described in the following table. The default poll interval is 5 seconds. To change the poll interval period, enter a new value in the Poll Interval field, and then click **Set Interval**. To stop polling, click **Stop**.

Table 72. IPSec VPN Connection Status screen information

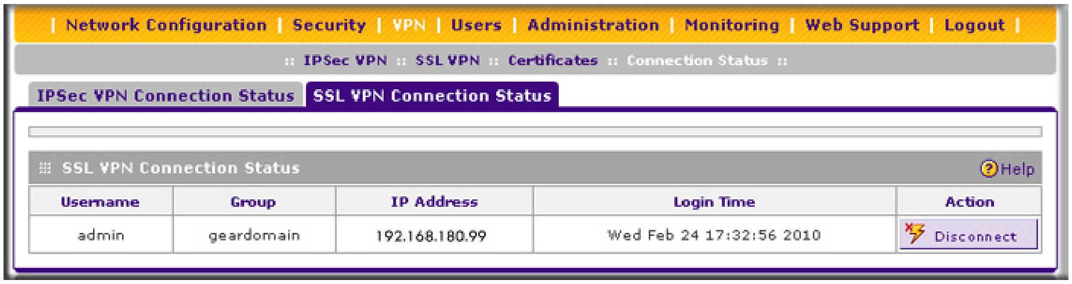
Item	Description
Policy Name	The name of the VPN policy that is associated with this SA.
Endpoint	The IP address on the remote VPN endpoint.

Table 72. IPSec VPN Connection Status screen information (continued)

Item	Description
Tx (KB)	The amount of data that is transmitted over this SA.
Tx (Packets)	The number of IP packets that are transmitted over this SA.
State	The current status of the SA. Phase 1 is the authentication phase, and Phase 2 is the key exchange phase. If there is no connection, the status is IPSec SA Not Established.
Action	Click the **Connect** table button to build the connection, or click the **Disconnect** table button to terminate the connection.

➤ To view the status of current SSL VPN tunnels:

Select **VPN > Connection Status > SSL VPN Connection Status**. The SSL VPN Connection Status screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: Certificates :: Connection Status ::
IPSec VPN Connection Status
SSL VPN Connection Status
Help

SSL VPN Connection Status

Username	Group	IP Address	Login Time	Action
admin	geardomain	192.168.180.99	Wed Feb 24 17:32:56 2010	Disconnect

Figure 171.

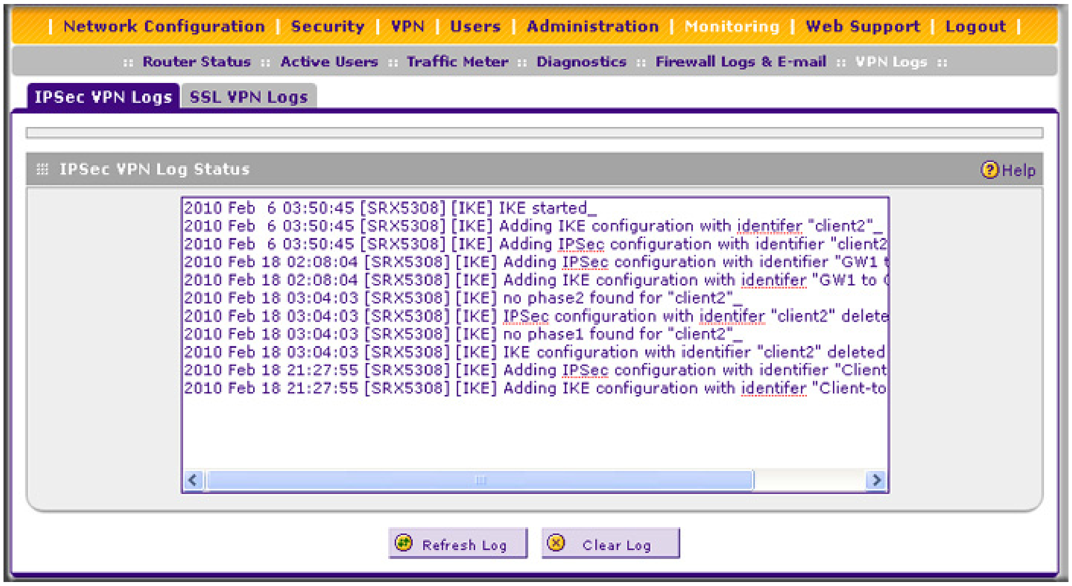
The active SSL VPN user’s user name, group, and IP address are listed in the table with a timestamp indicating the time and date that the user connected.

To disconnect an active user, click the **Disconnect** table button to the right of the user’s table entry.

View the VPN Logs

➤ To view the IPSec VPN logs:

Select **Monitoring > VPN Logs**. The VPN Logs submenu tabs display, with the IPSec VPN Logs screen in view:

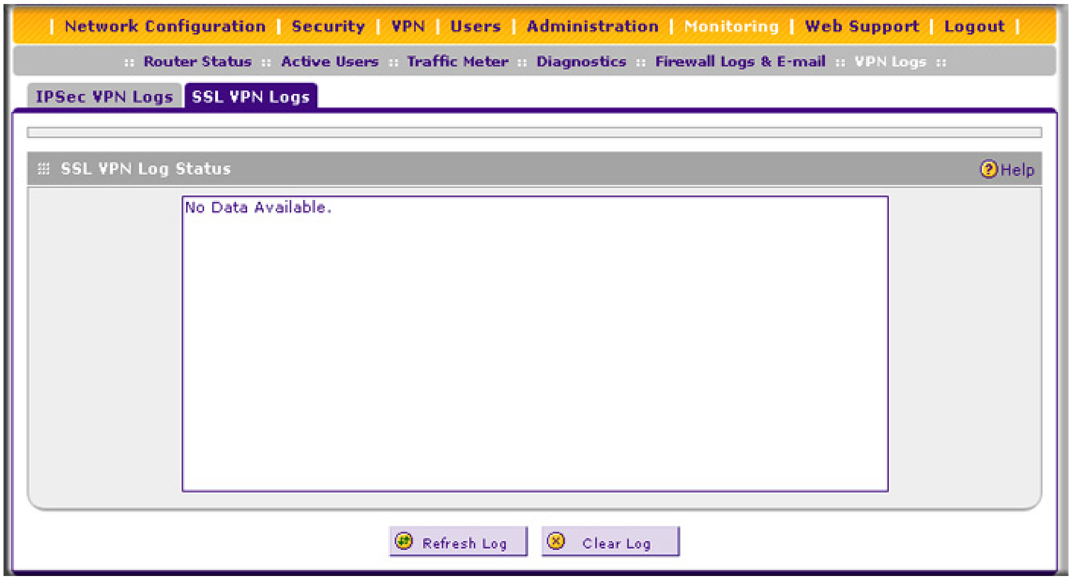

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
IPSec VPN Logs
SSL VPN Logs
IPSec VPN Log Status
Help
Refresh Log
Clear Log

```
2010 Feb  6 03:50:45 [SRX5308] [IKE] IKE started_
2010 Feb  6 03:50:45 [SRX5308] [IKE] Adding IKE configuration with identifer "client2"_
2010 Feb  6 03:50:45 [SRX5308] [IKE] Adding IPSec configuration with identifier "client2
2010 Feb 18 02:08:04 [SRX5308] [IKE] Adding IPSec configuration with identifier "GW1 t
2010 Feb 18 02:08:04 [SRX5308] [IKE] Adding IKE configuration with identifer "GW1 to (
2010 Feb 18 03:04:03 [SRX5308] [IKE] no phase2 found for "client2"_
2010 Feb 18 03:04:03 [SRX5308] [IKE] IPSec configuration with identifer "client2" delete
2010 Feb 18 03:04:03 [SRX5308] [IKE] no phase1 found for "client2"_
2010 Feb 18 03:04:03 [SRX5308] [IKE] IKE configuration with identifier "client2" deleted
2010 Feb 18 21:27:55 [SRX5308] [IKE] Adding IPSec configuration with identifier "Client
2010 Feb 18 21:27:55 [SRX5308] [IKE] Adding IKE configuration with identifer "Client-to
```

Figure 172.

➢ To view the SSL VPN log:

Select **Monitoring > VPN Logs > SSL VPN Logs**. The SSL VPN Logs screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
IPSec VPN Logs
SSL VPN Logs
SSL VPN Log Status
Help
Refresh Log
Clear Log

```
No Data Available.
```

Figure 173.

View the Port Triggering Status

➤ **To view the status of the port triggering feature:**

1. Select **Security > Port Triggering**. The Port Triggering screen displays (see *Figure 71* on page 131).
2. Click the **Status** option arrow in the upper right of the Port Triggering screen. The Port Triggering Status screen appears in a popup window:

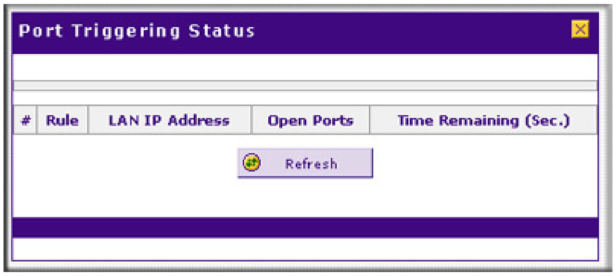

Port Triggering Status
# | Rule | LAN IP Address | Open Ports | Time Remaining (Sec.)
Refresh

Figure 174.

The Port Triggering Status screen displays the information that is described in the following table:

Table 73. Port Triggering Status screen information

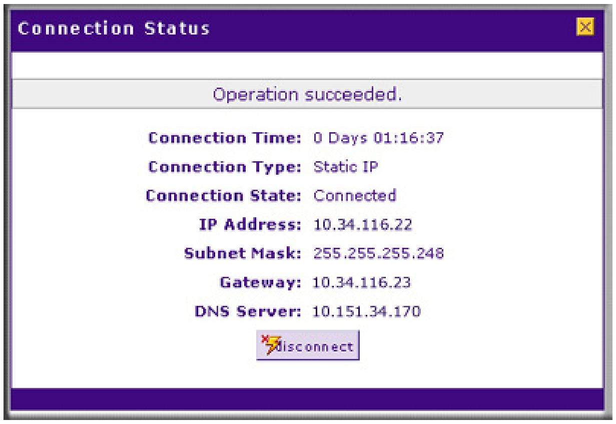
Item	Description
#	The sequence number of the rule onscreen.
Rule	The name of the port triggering rule that is associated with this entry.
LAN IP Address	The IP address of the computer or device that is currently using this rule.
Open Ports	The incoming ports that are associated with this rule. Incoming traffic using one of these ports is sent to the IP address that is listed in the LAN IP Address field.
Time Remaining	The time remaining before this rule is released and made available for other computers or devices. This timer is restarted when incoming or outgoing traffic is received.

View the WAN Port Connection Status

You can view the status of a WAN connection with its associated DNS servers and DHCP servers.

➤ **To view the status of a WAN connection:**

1. Select **Network Configuration > WAN Settings**. The WAN screen displays (see *Figure 10* on page 25).
2. Click the **Status** button in the Action column of the WAN interface for which you want to view the connection status. The Connection Status screen appears in a popup window:



Connection Status

Operation succeeded.

Connection Time: 0 Days 01:16:37
Connection Type: Static IP
Connection State: Connected
IP Address: 10.34.116.22
Subnet Mask: 255.255.255.248
Gateway: 10.34.116.23
DNS Server: 10.151.34.170

Figure 175.

The Connection Status screen displays the information that is described in the following table. The information that is shown on the Connection Status screen depends on the nature of the connection—static IP address or dynamically assigned IP address. Therefore, not all information that is described in the following table might be shown.

Table 74. WAN port Connection Status screen information

Item	Description
Connection Time	The period that the VPN firewall has been connected through the WAN port.
Connection Type	The connection type can be either DHCP or Static IP.
Connection Status	The connection status can be either Connected or Disconnected.
IP Address	The addresses that were automatically detected (see *Automatically Detecting and Connecting* on page 25) or that you have configured on the WAN ISP Settings screen (see *Manually Configure the Internet Connection* on page 28).
Subnet Mask	
Gateway	
DNS Server	
DHCP Server	The DHCP server that was automatically detected. This field is displayed only when your ISP does not require a login and the IP address is acquired dynamically from your ISP. You have configured these settings on the WAN ISP Settings screen (see *Manually Configure the Internet Connection* on page 28).
Lease Obtained	The time when the DHCP lease was obtained.
Lease Duration	The period that the DHCP lease remains in effect.

Depending on the type of connection, any of the following buttons might be displayed on the Connection Status screen:

- **Renew**. Click to renew the DHCP lease.
- **Release**. Click to disconnect the DHCP connection.
- **Disconnect**. Click to disconnect the static IP connection.

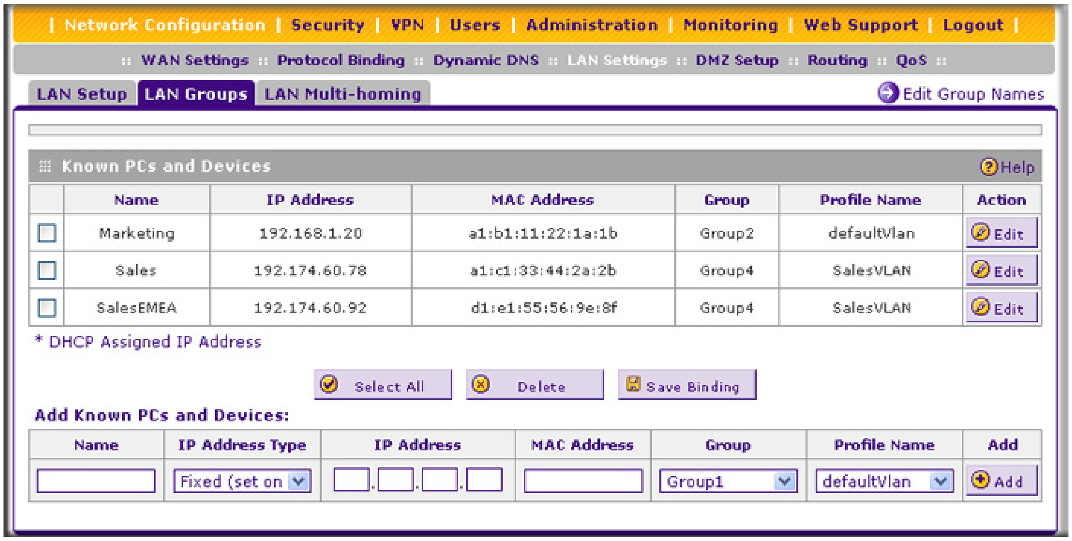
View the Attached Devices and DHCP Log

The LAN Groups screen shows the network database, which is the Known PCs and Devices table that contains all IP devices that the VPN firewall has discovered on the local network. The LAN Setup screen lets you access the DHCP log.

View Attached Devices

➤ **To view the network database:**

Select **Network Configuration > LAN Settings > LAN Groups**. The LAN Groups screen displays. (The following figure shows some examples in the Known PCs and Devices table.)


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
LAN Setup
LAN Groups
LAN Multi-homing
Edit Group Names
Help
Select All
Delete
Save Binding

Known PCs and Devices

	Name	IP Address	MAC Address	Group	Profile Name	Action
□	Marketing	192.168.1.20	a1:b1:11:22:1a:1b	Group2	defaultVlan	Edit
□	Sales	192.174.60.78	a1:c1:33:44:2a:2b	Group4	SalesVLAN	Edit
□	SalesEMEA	192.174.60.92	d1:e1:55:56:9e:8f	Group4	SalesVLAN	Edit

* DHCP Assigned IP Address

Add Known PCs and Devices:

Name	IP Address Type	IP Address	MAC Address	Group	Profile Name	Add
	Fixed (set on	. . .		Group1	defaultVlan	Add

Figure 176.

The Known PCs and Devices table contains a list of all known PCs and network devices that are assigned dynamic IP addresses by the VPN firewall, or have been discovered by other means. Collectively, these entries make up the network database.

For each PC or device, the following fields are displayed:

- **Check box**. Allows you to select the PC or device in the table.
- **Name**. The name of the PC or device. For computers that do not support the NetBIOS protocol, the name is displayed as Unknown (you can edit the entry manually to add a meaningful name). If the PC or device was assigned an IP address by the DHCP server, then the name is appended by an asterisk.
- **IP Address**. The current IP address of the PC or device. For DHCP clients of the VPN firewall, this IP address does not change. If a PC or device is assigned a static IP address, you need to update this entry manually after the IP address on the PC or device has changed.
- **MAC Address**. The MAC address of the PC or device's network interface.
- **Group**. Each PC or device can be assigned to a single LAN group. By default, a PC or device is assigned to Group 1. You can select a different LAN group from the Group

drop-down list in the Add Known PCs and Devices section or on the Edit Groups and Hosts screen (see *Figure 35* on page 70).

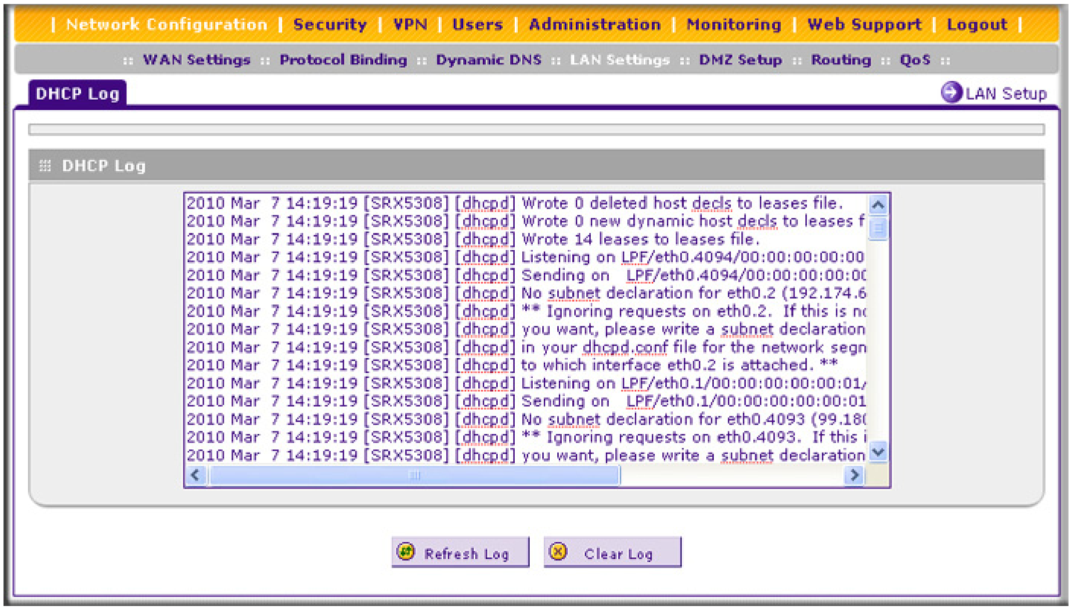
- **Profile Name**. The VLAN to which the PC or device is assigned.
- **Action**. The Edit table button that provides access to the Edit Groups and Hosts screen.

> **Note:** If the VPN firewall is rebooted, the data in the Known PCs and Devices table is lost until the VPN firewall rediscovers the devices.

View the DHCP Log

➢ To review the most recent entries in the DHCP log:

1. Select **Network Configuration > LAN Settings**. The LAN Settings submenu tabs display, with the LAN Setup screen in view (*Figure 30* on page 59).
2. Click the **DHCP Log** option arrow in the upper right of the LAN Setup screen. The DHCP Log screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing :: QoS ::
DHCP Log
LAN Setup
DHCP Log
Refresh Log
Clear Log

```
2010 Mar  7 14:19:19 [SRX5308] [dhcpd] Wrote 0 deleted host decls to leases file.
2010 Mar  7 14:19:19 [SRX5308] [dhcpd] Wrote 0 new dynamic host decls to leases f
2010 Mar  7 14:19:19 [SRX5308] [dhcpd] Wrote 14 leases to leases file.
2010 Mar  7 14:19:19 [SRX5308] [dhcpd] Listening on LPF/eth0.4094/00:00:00:00:00
2010 Mar  7 14:19:19 [SRX5308] [dhcpd] Sending on   LPF/eth0.4094/00:00:00:00:0(
2010 Mar  7 14:19:19 [SRX5308] [dhcpd] No subnet declaration for eth0.2 (192.174.6
2010 Mar  7 14:19:19 [SRX5308] [dhcpd] ** Ignoring requests on eth0.2.  If this is n(
2010 Mar  7 14:19:19 [SRX5308] [dhcpd] you want, please write a subnet declaration
2010 Mar  7 14:19:19 [SRX5308] [dhcpd] in your dhcpd.conf file for the network segn
2010 Mar  7 14:19:19 [SRX5308] [dhcpd] to which interface eth0.2 is attached. **
2010 Mar  7 14:19:19 [SRX5308] [dhcpd] Listening on LPF/eth0.1/00:00:00:00:00:01/
2010 Mar  7 14:19:19 [SRX5308] [dhcpd] Sending on   LPF/eth0.1/00:00:00:00:00:01
2010 Mar  7 14:19:19 [SRX5308] [dhcpd] No subnet declaration for eth0.4093 (99.18(
2010 Mar  7 14:19:19 [SRX5308] [dhcpd] ** Ignoring requests on eth0.4093.  If this i
2010 Mar  7 14:19:19 [SRX5308] [dhcpd] you want, please write a subnet declaration
```

Figure 177.

To view the most recent entries, click the **Refresh Log** button. To delete all the existing log entries, click the **Clear Log** button.

Use the Diagnostics Utilities

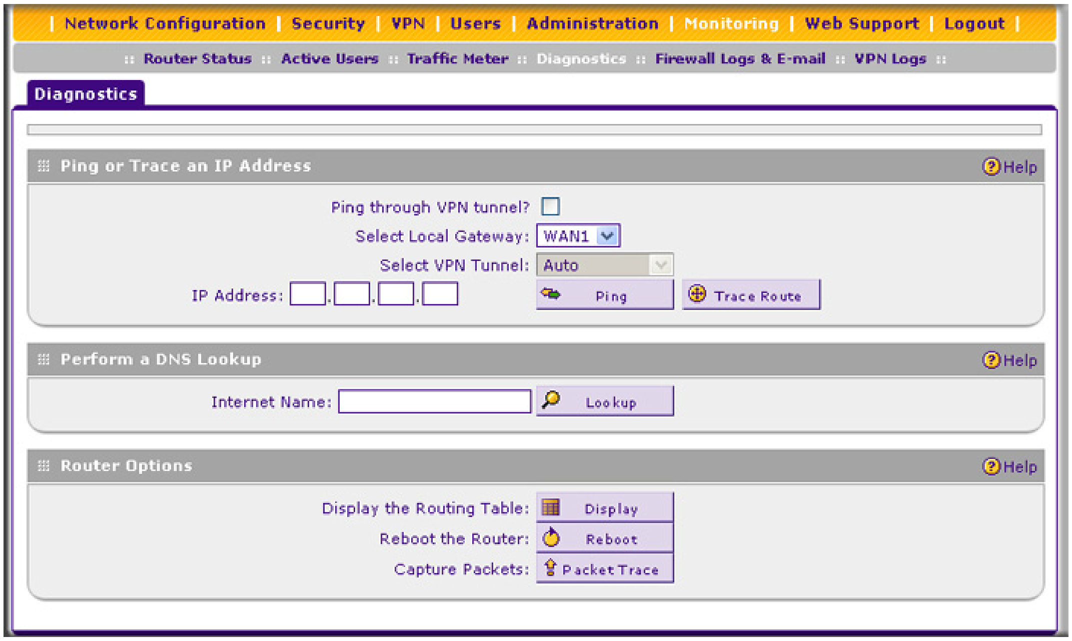
From the Diagnostics screen you can perform diagnostics that are discussed in the following sections:

- *Send a Ping Packet or Trace a Route*
- *Look Up a DNS Address*
- *Display the Routing Table*
- *Reboot the VPN Firewall*
- *Capture Packets*

> **Note:** For normal operation, diagnostics are not required.

➤ **To view the Diagnostics screen:**

Select **Monitoring > Diagnostics**. The Diagnostics screen displays:


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Diagnostics
Ping or Trace an IP Address
Help
Ping
Trace Route
Perform a DNS Lookup
Help
Lookup
Router Options
Help
Display
Reboot
Packet Trace

Ping through VPN tunnel? □

Select Local Gateway: WAN1

Select VPN Tunnel: Auto

IP Address: □.□.□.□

Internet Name: □

Display the Routing Table:

Reboot the Router:

Capture Packets:

Figure 178.

Send a Ping Packet or Trace a Route

Use the ping utility to perform one of the following diagnostic actions:

- Send a ping packet request to check the connection between the VPN firewall and a specific IP address. The ping results are displayed on the Ping screen; Click **Back** on the browser menu bar to return to the Diagnostics screen.

- Send a ping packet request to trace the route and to show the various hops between the VPN firewall and a specific IP address. The trace-route results are displayed on the Trace Route screen. Select **Monitoring > Diagnostics** to return to the Diagnostics screen.

If the request times out (no reply is received), it usually means that the destination is unreachable. However, some network devices can be configured not to respond to a ping.

➢ **To send a ping request:**

1. In the Ping or Trace and IP Address section on the Diagnostics screen, make one of the following selections to specify how the destination should be reached:
   - If the specified address is reached through a VPN tunnel:
     a. Select the **Ping through VPN tunnel** check box.
     b. Select either **Auto** or a specific VPN tunnel from the Select VPN Tunnel drop-down list.
   - If the specified address is not reached through a VPN tunnel, select a WAN interface from the Select Local Gateway drop-down list.
2. In the **IP Address** field, enter the IP address that you want to ping.
3. Make one of the following selections:
   - Click the **Ping** button. The results are displayed on the Ping screen. To return to the Diagnostics screen, click **Back** on the browser menu bar.
   - Click the **Trace Route** button. The results are displayed on the Trace Route screen. Select **Monitoring > Diagnostics** to return to the Diagnostics screen.

Look Up a DNS Address

A DNS (Domain Name Server) converts the Internet name (for example, www.netgear.com) to an IP address. If you need the IP address of a web, FTP, mail, or other server on the Internet, request a DNS lookup to find the IP address.

➢ **To look up a DNS address:**

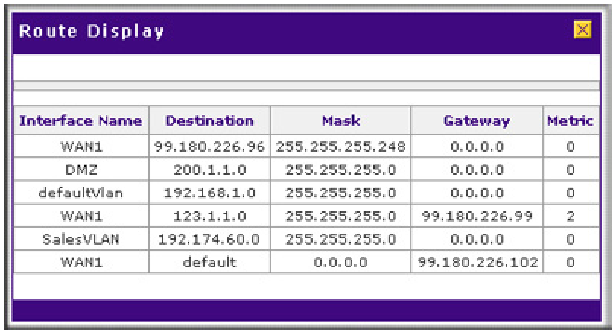
1. In the Perform a DNS Lookup section on the Diagnostics screen, enter a domain name in the **Internet Name** field.
2. Click the **Lookup** button. The results of the lookup action are displayed in the NS Lookup screen. To return to the Diagnostics screen, click **Back** on the browser menu bar.

Display the Routing Table

Displaying the internal routing table can assist NETGEAR technical support in diagnosing routing problems.

➢ **To display the routing table:**

In the Router Options section on the Diagnostics screen, next to Display the Routing Table, click the **Display** button. The routing table is displayed in the Route Display screen that appears as a popup window. (The IP addresses that are shown in the following figure do not relate to other figures and examples in this manual.)



Route Display

Interface Name	Destination	Mask	Gateway	Metric
WAN1	99.180.226.96	255.255.255.248	0.0.0.0	0
DMZ	200.1.1.0	255.255.255.0	0.0.0.0	0
defaultVlan	192.168.1.0	255.255.255.0	0.0.0.0	0
WAN1	123.1.1.0	255.255.255.0	99.180.226.99	2
SalesVLAN	192.174.60.0	255.255.255.0	0.0.0.0	0
WAN1	default	0.0.0.0	99.180.226.102	0

Figure 179.

Reboot the VPN Firewall

You can perform a remote reboot (restart), for example, when the VPN firewall seems to have become unstable or is not operating normally.

Note: Rebooting breaks any existing connections either to the VPN firewall (such as your management session) or through the VPN firewall (for example, LAN users accessing the Internet). However, when the reboot process is complete, connections to the Internet are automatically reestablished if possible.

➤ **To reboot the VPN firewall:**

In the Router Options section on the Diagnostics screen, next to Reboot the Router, click the **Reboot** button. The VPN firewall reboots. (If you can see the unit: the reboot process is complete when the Test LED on the front panel goes off.)

Capture Packets

You can capture packets to analyze traffic patterns with a network traffic analyzer tool. The captured packet flow can show if traffic is flowing correctly to its destinations or if packets are dropped. There is a limit to the size of the packet flow that you can capture in a file.

➤ **To capture packets:**

1. In the Router Options section on the Diagnostics screen, next to Capture Packets, click the **Packet Trace** button. The Capture Packets screen appears as a popup window:

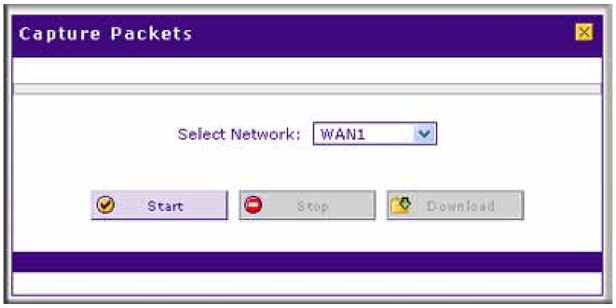


Figure 180.

2. From the **Select Network** drop-down list, select a WAN interface, DMZ interface (if enabled), or VLAN.
3. Click the **Start** button to start capturing the traffic flow. The following text appears in the popup window: *Packet tracing started. Click "stop" when done*.
4. When you want to stop capturing the traffic flow, click the **Stop** button. The following text appears in the popup window: *Packet tracing stopped. Click "download" to view captured logs*.
5. Click the **Download** button. Select a location to save the captured traffic flow. (The default file name is pkt.CAP.) The file is downloaded to the location that you specify.
6. Send the file to NETGEAR technical support for analysis.

10. Troubleshooting and Using Online Support 10

This chapter provides troubleshooting tips and information for the VPN firewall. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the VPN firewall on?

  Go to *Basic Functioning* on page 294.
- Have I connected the VPN firewall correctly?

  Go to *Basic Functioning* on page 294.
- I cannot access the VPN firewall's web management interface.

  Go to *Troubleshoot the Web Management Interface* on page 295.
- A time-out occurs.

  Go to *When You Enter a URL or IP Address a Time-Out Error Occurs* on page 296.
- I cannot access the Internet or the LAN.

  Troubleshoot the ISP Connection on page 296.
- I have problems with the LAN connection.

  Go to *Troubleshoot a TCP/IP Network Using the Ping Utility* on page 298.
- I want to clear the configuration and start over again.

  Go to *Restore the Default Configuration and Password* on page 299.
- The date or time is not correct.

  Go to *Problems with Date and Time* on page 300.
- I need help from NETGEAR.

  Go to *Access the Knowledge Base and Documentation* on page 301.

Note: The VPN firewall's diagnostic tools are explained in *Use the Diagnostics Utilities* on page 289.

Basic Functioning

After you turn on power to the VPN firewall, the following sequence of events should occur:

1. When power is first applied, verify that the Power LED is on.
2. After approximately 2 minutes, verify that:
   - **a.** The Test LED is no longer lit.
   - **b.** The left LAN port LEDs are lit for any local ports that are connected.
   - **c.** The left WAN port LEDs are lit for any WAN ports that are connected.

   If a port's left LED is lit, a link has been established to the connected device. If a port is connected to a 1000 Mbps device, verify that the port's right LED is green. If the port functions at 100 Mbps, the right LED is amber. If the port functions at 10 Mbps, the right LED is off.

If any of these conditions do not occur, see the appropriate following section.

Power LED Not On

If the Power and other LEDs are off when your VPN firewall is turned on, make sure that the power cord is correctly connected to your VPN firewall and that the power supply adapter is correctly connected to a functioning power outlet.

If the error persists, you have a hardware problem and should contact NETGEAR Technical Support.

Test LED Never Turns Off

When the VPN firewall is powered on, the Test LED turns on for approximately 2 minutes and then turns off when the VPN firewall has completed its initialization. If the Test LED remains on, there is a fault within the VPN firewall.

If all LEDs are still on more than several minutes minute after power up:

- Turn the power off, and then turn it on again to see if the VPN firewall recovers.
- Reset the VPN firewall's configuration to factory defaults. Doing so sets the VPN firewall's IP address to **192.168.1.1**. This procedure is explained in *Restore the Default Configuration and Password* on page 299.

If the error persists, you might have a hardware problem and should contact NETGEAR Technical Support.

LAN or WAN Port LEDs Not On

If either the LAN LEDs or WAN LEDs do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the VPN firewall and at the hub, router, or workstation.
- Make sure that power is turned on to the connected hub, router, or workstation.
- Be sure you are using the correct cables:

  When connecting the VPN firewall's WAN ports to one or two devices that provide the Internet connections, use the cables that are supplied with the devices. These cables could be a standard straight-through Ethernet cables or an Ethernet crossover cables.

Troubleshoot the Web Management Interface

If you are unable to access the VPN firewall's web management interface from a PC on your local network, check the following:

- Check the Ethernet connection between the PC and the VPN firewall as described in the previous section (*LAN or WAN Port LEDs Not On*).
- Make sure your PC's IP address is on the same subnet as the VPN firewall. If you are using the recommended addressing scheme, your PC's address should be in the range of 192.168.1.2 to 192.168.1.254.

Note: If your PC's IP address is shown as 169.254.x.x:
Windows and Mac operating systems generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the PC to the VPN firewall and reboot your PC.

- If your VPN firewall's IP address has been changed and you do not know the current IP address, reset the VPN firewall's configuration to factory defaults. This sets the VPN firewall's IP address to **192.168.1.1**. This procedure is explained in *Restore the Default Configuration and Password* on page 299.

  Tip: If you do not want to revert to the factory default settings and lose your configuration settings, you can reboot the VPN firewall and use a sniffer to capture packets sent during the reboot. Look at the ARP packets to locate the VPN firewall's LAN interface address.

- Make sure that you are using the SSL https://address login rather than the http://address login.

- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when entering this information.

If the VPN firewall does not save changes you have made in the web management interface, check the following:

- When entering configuration settings, be sure to click the **Apply** button before moving to another menu or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser. The changes might have occurred, but the web browser might be caching the old configuration.

When You Enter a URL or IP Address a Time-Out Error Occurs

A number of things could be causing this situation. Try the following troubleshooting steps.

- Check whether other computers on the LAN work correctly. If they do, ensure that your computer's TCP/IP settings are correct. If you use a fixed (static) IP address, check the subnet mask, default gateway, DNS, and IP addresses on the WAN ISP Settings screens (see *Manually Configure the Internet Connection* on page 28).
- If the computer is configured correctly, but still not working, ensure that the VPN firewall is connected and turned on. Connect to the web management interface and check the VPN firewall's settings. If you cannot connect to the VPN firewall, see the information in the previous section (*Troubleshoot the Web Management Interface* on page 295).
- If the VPN firewall is configured correctly, check your Internet connection (for example, your modem or router) to make sure that it is working correctly.

Troubleshoot the ISP Connection

If your VPN firewall is unable to access the Internet, you should first determine whether the VPN firewall is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your VPN firewall requests an IP address from the ISP. You can determine whether the request was successful using the web management interface.

To check the WAN IP address for a WAN interface:

1. Launch your browser and navigate to an external site such as www.netgear.com.
2. Access the web management interface of the VPN firewall's configuration at https://192.168.1.1.
3. Select **Network Configuration> WAN Settings**. The WAN Settings screen displays.

4. Click the **Status** button in the Action column of the WAN interface for which you want to view the connection status. The Connection Status screen appears in a popup window. (For more information, see *View the WAN Port Connection Status* on page 285.)
5. Check that an IP address is shown for the WAN port.
   If 0.0.0.0 is shown, your VPN firewall has not obtained an IP address from your ISP.

If your VPN firewall is unable to obtain an IP address from the ISP, you might need to force your modem or router to recognize your new VPN firewall by performing the following procedure:

1. Turn off the power to the modem or router.
2. Turn off the power to your VPN firewall.
3. Wait 5 minutes, and then turn on the power to the modem or router.
4. When the modem's or router's LEDs indicate that it has reacquired synchronization with the ISP, turn on the power to your VPN firewall.

If your VPN firewall is still unable to obtain an IP address from the ISP, the problem might be one of the following:

- Your ISP might require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, you might have incorrectly set the login name and password.
- Your ISP might check for your PC's host name.
  Enter the host name, system name, or account name that was assigned to you by your ISP in the Account Name field on the WAN ISP Settings screen for the WAN interface that you are troubleshooting. You might also have to enter the assigned domain name or workgroup name in the Domain Name field, and you might have to enter additional information (see *Manually Configure the Internet Connection* on page 28).
- Your ISP allows only one Ethernet MAC address to connect to the Internet, and might check for your PC's MAC address. In this case, do one of the following:
  - Inform your ISP that you have bought a new network device, and ask them to use the VPN firewall's MAC address.
  - Configure your VPN firewall to spoof your PC's MAC address. You can do this in the Router's MAC Address section of the WAN Advanced Options screen for the WAN interface that you are troubleshooting (see *Configure Advanced WAN Options* on page 51).

If your VPN firewall can obtain an IP address, but an attached PC is unable to load any web pages from the Internet:

- Your PC might not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www.netgear.com) to numeric IP addresses. Typically your ISP provides the addresses of one or two DNS servers for your use. You can configure your PC manually with DNS addresses, as explained in your operating system documentation.
- Your PC might not have the VPN firewall configured as its TCP/IP gateway.

Troubleshoot a TCP/IP Network Using the Ping Utility

Most TCP/IP terminal devices and firewalls contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshoot a TCP/IP network by using the ping utility in your PC or workstation.

Test the LAN Path to Your VPN Firewall

You can ping the VPN firewall from your PC to verify that the LAN path to the VPN firewall is set up correctly.

To ping the VPN firewall from a PC running Windows 95 or later:

1. From the Windows toolbar, click **Start** and select **Run**.
2. In the field provided, type **`ping`** followed by the IP address of the VPN firewall; for example:

   ```
   ping 192.168.1.1
   ```

3. Click **OK**. A message, similar to the following, should display:

   ```
   Pinging <IP address> with 32 bytes of data
   ```

   If the path is working, you will see this message:

   ```
   Reply from <IP address>: bytes=32 time=NN ms TTL=xxx
   ```

   If the path is not working, you will see this message:

   ```
   Request timed out
   ```

   If the path is not functioning correctly, you could have one of the following problems:

   - Wrong physical connections
     - Make sure that the LAN port LED is on. If the LED is off, follow the instructions in *LAN or WAN Port LEDs Not On* on page 295.
     - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and VPN firewall.
   - Wrong network configuration
     - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
     - Verify that the IP address for your VPN firewall and your workstation are correct and that the addresses are on the same subnet.

Test the Path from Your PC to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device. From the Windows run menu, type:

```
ping -n 10 <IP address>
```

where <*IP address*> is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- Check that your PC has the IP address of your VPN firewall listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information is not visible in your PC's Network Control Panel.
- Check to see that the network address of your PC (the portion of the IP address that is specified by the netmask) is different from the network address of the remote device.
- Check that the modem or router is connected and functioning.
- If your ISP assigned a host name, system name, or account name to your PC, enter that name in the Account Name field on the WAN ISP Settings screen for the WAN interface that you are troubleshooting. You might also have to enter the assigned domain name or workgroup name in the Domain Name field, and you might have to enter additional information (see *Manually Configure the Internet Connection* on page 28).
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you need to configure your VPN firewall to clone or spoof the MAC address from the authorized PC. You can do this in the Router's MAC Address section of the WAN Advanced Options screen for the WAN interface that you are troubleshooting (see *Configure Advanced WAN Options* on page 51).

Restore the Default Configuration and Password

To reset the VPN firewall to the original factory default settings, you can use one of the following two methods:

- Push the reset button on the rear panel of the VPN firewall (see *Rear Panel* on page 16) and hold the reset button for about 8 seconds until the Test LED turns on and begins to blink (about 30 seconds). To restore the factory default configuration settings when you do not know the administration password or IP address, you need to use the reset button method.
- On the Settings Backup and Firmware Upgrade screen, next to Revert to factory default settings, click the **Default** button:

  a. To display the Settings Backup and Firmware Upgrade screen, select **Administration > Settings Backup and Firmware Upgrade** (see the following figure).

  b. Click the **Default** button.

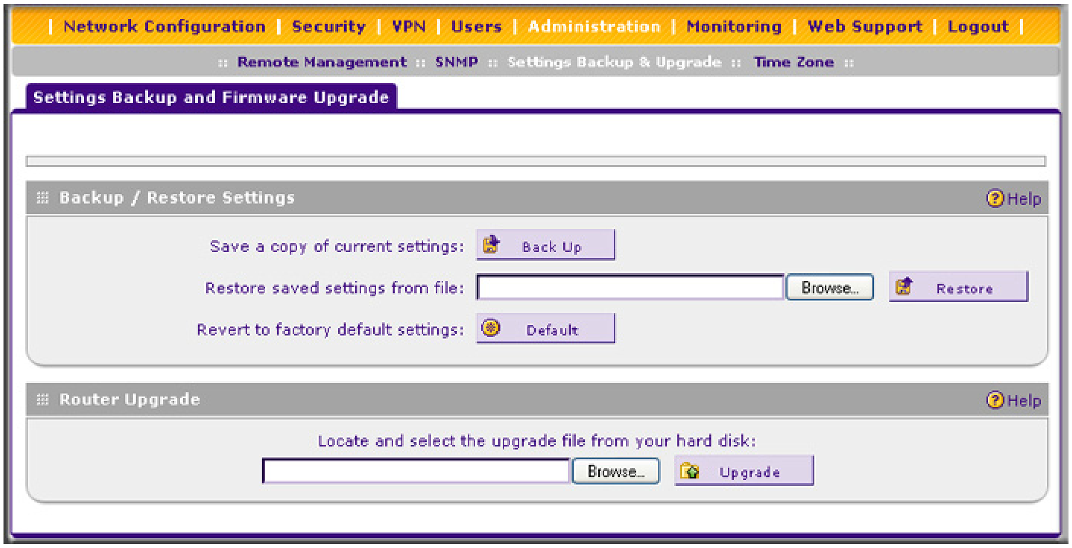

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone ::
Settings Backup and Firmware Upgrade
Backup / Restore Settings
Help
Save a copy of current settings:
Back Up
Restore saved settings from file:
Browse...
Restore
Revert to factory default settings:
Default
Router Upgrade
Help
Locate and select the upgrade file from your hard disk:
Browse...
Upgrade

Figure 181.

The VPN firewall reboots. During the reboot process, the Settings Backup and Firmware Upgrade screen might remain visible. The reboot process is complete after several minutes when the Test LED on the front panel goes off.

WARNING!

When you push the hardware reset button or click the software Default button, the VPN firewall settings are erased. All firewall rules, VPN policies, LAN/WAN settings, and other settings are lost. Back up your settings if you intend on using them.

Note: After rebooting with factory default settings, the VPN firewall's password is **password**, and the LAN IP address is **192.168.1.1**.

Problems with Date and Time

The Time Zone screen displays the current date and time of day (see *Configure Date and Time Service* on page 260). The VPN firewall uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day.

Problems with the date and time function can include:

- Date shown is January 1, 2000. Cause: The VPN firewall has not yet successfully reached a network time server. Check that your Internet access settings are configured correctly. If you have just completed configuring the VPN firewall, wait at least 5 minutes and check the date and time again.

- Time is off by 1 hour. Cause: The VPN firewall does not automatically sense daylight savings time. Go to the Time Zone screen, and select or clear the **Automatically Adjust for Daylight Savings Time** check box.

Access the Knowledge Base and Documentation

To access NETGEAR's knowledge base for the VPN firewall, select **Web Support > Knowledgebase**. To access NETGEAR's documentation library for the VPN firewall, select Web **Support > Documentation**.

Default Settings and Technical Specifications

A

You can use the reset button located on the rear panel to reset all settings to their factory defaults. This is called a hard reset (for more information, see *Revert to Factory Default Settings* on page 258).

- To perform a hard reset, press and hold the reset button for approximately 8 seconds (until the Test LED blinks rapidly). The VPN firewall returns to the factory configuration settings that are shown in the following table.
- Pressing the reset button for a shorter period of time simply causes the VPN firewall to reboot.

The following table shows the default configuration settings for the VPN firewall:

Table 75. VPN firewall default configuration settings

Feature		Default behavior
Router login		
	User login URL	https://192.168.1.1
	Administrator user name (case-sensitive)	admin
	Administrator login password (case-sensitive)	password
	Guest user name (case-sensitive)	guest
	Guest login password (case-sensitive)	password
Internet connection		
	WAN MAC address	Use default address
	WAN MTU size	1500
	Port speed	10/100/1000 AutoSense
Local network (LAN)		
	LAN IP address	192.168.1.1
	Subnet mask	255.255.255.0
	RIP direction	None
	RIP version	Disabled

Table 75. VPN firewall default configuration settings (continued)

Feature		Default behavior
(continued)	RIP authentication	Disabled
	DHCP server	Enabled
	DHCP starting IP address	192.168.1.2
	DHCP starting IP address	192.168.1.100
Management		
	Time zone	GMT
	Time zone adjusted for daylight savings time	Disabled
	SNMP	Disabled
	Remote management	Disabled
Firewall		
	Inbound (communications coming in from the Internet)	All communication denied
	Outbound (communications from the LAN to the Internet)	All communication allowed
	Source MAC filtering	Disabled
	Stealth mode	Enabled
	Respond to ping on Internet ports	Disabled

The following table shows the physical and technical specifications for the VPN firewall:

Table 76. VPN firewall physical and technical specifications

Feature			Specification
Network protocol and standards compatibility			
	Data and Routing Protocols		TCP/IP, RIP-1, RIP-2, DHCP PPP over Ethernet (PPPoE)
Power adapter			
	Universal input		100–240V, AC/50–60 Hz, 1.2 Amp maximum
Physical specifications			
	Dimensions (W x H x D)	cm	33 x 4.3 x 20.9
		inches	13 x 1.7 x 8.2
	Weight	kg	2.1
		lb.	4.6

Table 76. VPN firewall physical and technical specifications (continued)

Feature			Specification
Environmental specifications			
	Operating temperatures	C	0º to 45º
		F	32º to 113º
	Storage temperatures	C	–20º to 70º
		F	–4º to 158º
	Operating humidity		90% maximum relative humidity, noncondensing
	Storage humidity		95% maximum relative humidity, noncondensing
Major regulatory compliance			
	Meets requirements of		FCC Class A
			CE
			WEEE
			RoHS
Interface specifications			
	4 LAN, one of which is a configurable DMZ interface		AutoSense 10/100/1000BASE-T, RJ-45
	4 WAN		AutoSense 10/100/1000BASE-T, RJ-45
	1 administrative console port		RS-232

The following table shows the IPSec VPN specifications for the VPN firewall:

Table 77. VPN firewall IPSec VPN specifications

Setting	Specification
Network Management	Web-based configuration and status monitoring
Number of concurrent users supported	125
IPSec encryption algorithm	DES, 3DES, AES-128, AES-192, AES-256
IPSec authentication algorithm	SHA-1, MD5
IPSec key exchange	IKE, Manual Key, Pre-Shared Key, PKI, X.500
IPSec authentication types	Local user database, RADIUS PAP, RADIUS CHAP
IPSec certificates supported	CA digital certificate, self-signed certificate

The following table shows the SSL VPN specifications for the VPN firewall:

Table 78. VPN firewall SSL VPN specifications

Setting	Specification
Network Management	Web-based configuration and status monitoring
Number of concurrent users supported	50
SSL versions	SSLv3, TLS1.0
SSL encryption algorithm	DES, 3DES, ARC4, AES-128, AES-192, AES-256
SSL message integrity	MD5, SHA-1, MAC-MD5/SHA-1, HMAC-MD5/SHA-1
SSL authentication types	Local user database, RADIUS-PAP, RADIUS-CHAP, RADIUS-MSCHAP, RADIUS-MSCHAPv2, WIKI-PAP, WiKID-CHAP, MIAS-PAP, MIAS-CHAP, NT domain
SSL certificates supported	CA digital certificate, self-signed certificate

Network Planning for Multiple WAN Ports

B

This appendix describes the factors to consider when planning a network using a firewall that has more than one WAN port.

This appendix contains the following sections:

- *What to Consider Before You Begin*
- *Overview of the Planning Process*
- *Inbound Traffic*
- *Virtual Private Networks*

What to Consider Before You Begin

The VPN firewall is a powerful and versatile solution for your networking needs. To make the configuration process easier and to understand all of the choices that are available to you, consider the following before you begin:

1. Plan your network.
   - **a.** Determine whether you will use one or several WAN ports. For one WAN port, you might need a fully qualified domain name either for convenience or to remotely access a dynamic WAN IP address.
   - **b.** If you intend to use several WAN ports, determine whether you will use them in auto-rollover mode for increased system reliability or load balancing mode for maximum bandwidth efficiency. See the topics in this appendix for more information. Your decision has the following implications:
     - Fully qualified domain name (FQDN)
       - For auto-rollover mode, you will need an FQDN to implement features such as exposed hosts and virtual private networks.
       - For load balancing mode, you might still need an FQDN either for convenience or to remotely access a dynamic WAN IP address.
     - Protocol binding.
       - For auto-rollover mode, protocol binding does not apply.
       - For load balancing mode, decide which protocols should be bound to a specific WAN port.
       - You can also add your own service protocols to the list.

2. Set up your accounts.
   a. Obtain active Internet services such a DSL broadband accounts and locate the Internet Service Provider (ISP) configuration information.
      - In this manual, the WAN side of the network is presumed to be provisioned as shown in the following figure, with two ISPs connected to the VPN firewall through separate physical facilities.
      - Each WAN port needs to be configured separately, whether you are using a separate ISP for each WAN port or you are using the same ISP to route the traffic of both WAN ports.

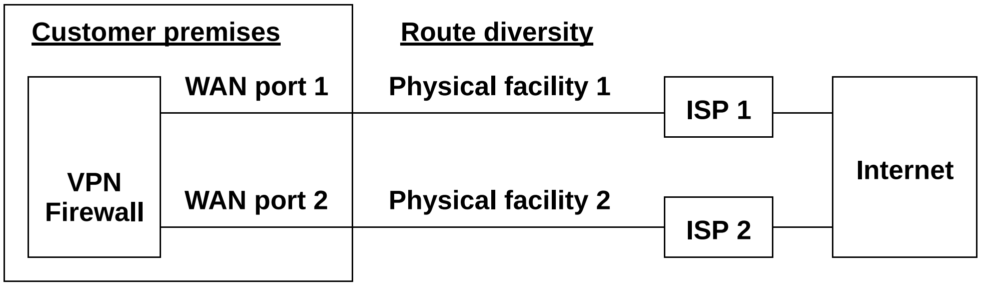


Figure 182.

      - If your ISP charges by the volume of data traffic each month, consider enabling the VPN firewall's traffic meter to monitor or limit your traffic.

   b. Contact a Dynamic DNS service and register FQDNs for one or both WAN ports.
3. Plan your network management approach.
   - The VPN firewall is capable of being managed remotely, but this feature needs to be enabled locally after each factory default reset.

     NETGEAR strongly advises you to change the default management password to a strong password before enabling remote management.
   - You can choose a variety of WAN options if the factory default settings are not suitable for your installation. These options include enabling a WAN port to respond to a ping, and setting MTU size, port speed, and upload bandwidth.
4. Prepare to physically connect the firewall to your cable or DSL modems and a computer. Instructions for connecting the VPN firewall are in the *ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308 Installation Guide*.

Cabling and Computer Hardware Requirements

For you to use the VPN firewall in your network, each computer needs to have an Ethernet network interface card (NIC) installed and needs to be equipped with an Ethernet cable. If the computer will connect to your network at 100 Mbps or higher speeds, you need to use a Category 5 (Cat5) cable.

Computer Network Configuration Requirements

The VPN firewall integrates a web management interface. To access the configuration screens on the VPN firewall, you need to use a Java-enabled web browser that supports HTTP uploads such as Microsoft Internet Explorer 6 or later, Mozilla Firefox 3 or later, or Apple Safari 3 or later with JavaScript, cookies, and SSL enabled. Free browsers are readily available for Windows, Macintosh, and UNIX/Linux.

For the initial connection to the Internet and configuration of the VPN firewall, you need to connect a computer to the VPN firewall, and the computer needs to be configured to automatically get its TCP/IP configuration from the VPN firewall via DHCP.

The cable or DSL modem broadband access device needs to provide a standard 10 Mbps (10BASE-T) Ethernet interface.

Internet Configuration Requirements

Depending on how your ISP sets up your Internet accounts, you will need the following Internet configuration information to connect VPN firewall to the Internet:

- Host and domain names
- One or more ISP login names and passwords
- ISP Domain Name Server (DNS) addresses
- One or more fixed IP addresses (also known as static IP addresses)

Where Do I Get the Internet Configuration Information?

There are several ways you can gather the required Internet connection information.

Your ISPs provide all the information needed to connect to the Internet. If you cannot locate this information, you can ask your ISP to provide you with it, or, if you have a computer already connected using the active Internet access account, you can gather the configuration information from that computer.

- For Windows 95/98/ME, open the Network Control Panel, select the TCP/IP entry for the Ethernet adapter, and click Properties. Record all the settings for each tab page.
- For Windows 2000/XP/Vista, open the Local Area Network Connection, select the TCP/IP entry for the Ethernet adapter, and click Properties. Record all the settings for each tab page.
- For Macintosh computers, open the TCP/IP or Network Control Panel. Record all the settings for each section.

After you have located your Internet configuration information, you might want to record the information in the following section.

Internet Connection Information

Print this page with the Internet connection information. Fill in the configuration settings that are provided to you by ISP.

- **ISP Login Name:** The login name and password are case-sensitive and need to be entered exactly as given by your ISP. For AOL customers, the login name is their primary screen name. Some ISPs use your full email address as the login name. The service name is not required by all ISPs. If you connect using a login name and password, then fill in the following:

  Login Name: ______________________________

  Password: ______________________________

  Service Name: ______________________________

- **Fixed or Static IP Address:** If you have a static IP address, record the following information. For example, 169.254.141.148 could be a valid IP address.

  Fixed or Static Internet IP Address : ______.______.______.______

  Gateway IP Address: ______.______.______.______

  Subnet Mask: ______.______.______.______

- **ISP DNS Server Addresses:** If you were given DNS server addresses, fill in the following:

  Primary DNS Server IP Address: ______.______.______.______

  Secondary DNS Server IP Address: ______.______.______.______

- **Host and Domain Names:** Some ISPs use a specific host or domain name such as CCA7324-A or home. If you have not been given host or domain names, you can use the following examples as a guide:
  - If your main email account with your ISP is aaa@yyy.com, then use **aaa** as your host name. Your ISP might call this your account, user, host, computer, or system name.
  - If your ISP's mail server is mail.xxx.yyy.com, then use **xxx.yyy.com** as the domain name.

  ISP Host Name: ________________________

  ISP Domain Name: ________________________

- **Fully Qualified Domain Name:** Some organizations use a fully qualified domain name (FQDN) from a Dynamic DNS service provider for their IP addresses.

  Dynamic DSN Service Provider: ________________________

  FQDN: ________________________

Overview of the Planning Process

The areas that require planning when you use a firewall that has multiple WAN ports such as the VPN firewall include the following:

- Inbound traffic (port forwarding, port triggering)
- Outbound traffic (protocol binding)
- Virtual private networks (VPNs)

Two WAN ports can be configured on a mutually exclusive basis to either of the following:

- auto-rollover for increased reliability
- load balance for outgoing traffic

These various types of traffic and auto-rollover or load balancing all interact to make the planning process more challenging:

- **Inbound traffic**. Unrequested incoming traffic can be directed to a PC on your LAN rather than being discarded. The mechanism for making the IP address public depends on whether the dual WAN ports are configured for auto-rollover or load balancing.
- **Virtual private networks**. A virtual private network (VPN) tunnel provides a secure communication channel either between two gateway VPN firewalls or between a remote PC client and gateway VPN firewall. As a result, the IP address of at least one of the tunnel endpoints needs to be known in advance in order for the other tunnel end point to establish (or reestablish) the VPN tunnel.

Note: When the VPN firewall’s WAN port rolls over, the VPN tunnel closes and needs to be reestablished using the new WAN IP address. However, you can configure automatic IPSec VPN rollover to ensure that an IPSec VPN tunnel is reestablished.

- **Dual WAN ports in auto-rollover mode**. Rollover for a VPN firewall with dual WAN ports is different from a single WAN port gateway configuration when you specify the IP address. Only one WAN port is active at a time, and when it rolls over, the IP address of the active WAN port always changes. Therefore, the use of a fully qualified domain name (FQDN) is always required, even when the IP address of each WAN port is fixed.

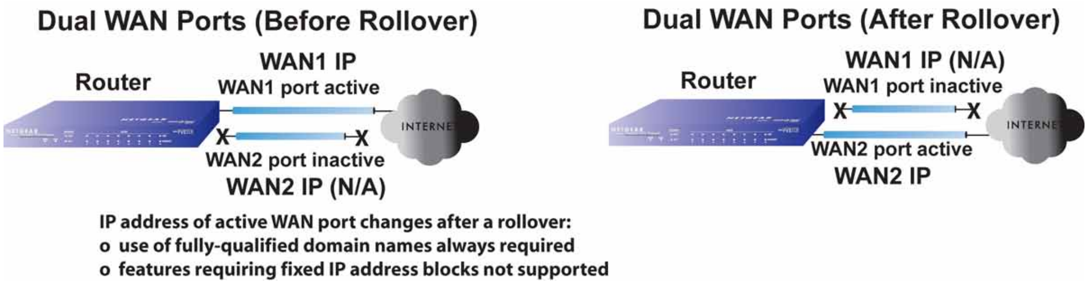

Dual WAN Ports (Before Rollover)
Router
WAN1 IP
WAN1 port active
INTERNET
WAN2 port inactive
WAN2 IP (N/A)
IP address of active WAN port changes after a rollover:
o use of fully-qualified domain names always required
o features requiring fixed IP address blocks not supported
Dual WAN Ports (After Rollover)
Router
WAN1 IP (N/A)
WAN1 port inactive
INTERNET
WAN2 port active
WAN2 IP

Figure 183.

Features such as multiple exposed hosts are not supported in auto-rollover mode because the IP addresses of each WAN port needs to be in the identical range of fixed addresses.

- **Dual WAN ports in load balancing mode**. Load balancing for a VPN firewall with dual WAN ports is similar to a single WAN gateway configuration when you specify the IP address. Each IP address is either fixed or dynamic based on the ISP: You need to use FQDNs when the IP address is dynamic, but FQDNs are optional when the IP address is static.

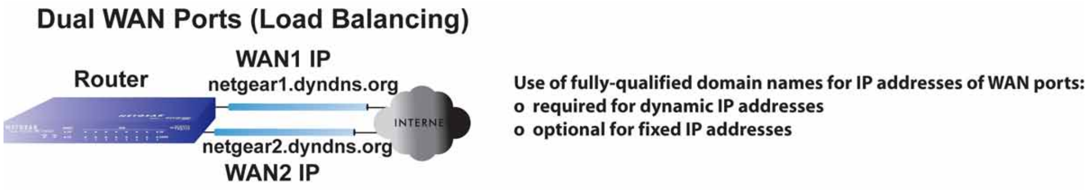

Dual WAN Ports (Load Balancing)
Router
WAN1 IP
netgear1.dyndns.org
INTERNET
netgear2.dyndns.org
WAN2 IP
Use of fully-qualified domain names for IP addresses of WAN ports:
o required for dynamic IP addresses
o optional for fixed IP addresses

Figure 184.

Inbound Traffic

Incoming traffic from the Internet is normally discarded by the VPN firewall unless the traffic is a response to one of your local computers or a service for which you have configured an inbound rule. Instead of discarding this traffic, you can configure the VPN firewall to forward it to one or more LAN hosts on your network.

The addressing of the VPN firewall's dual WAN port depends on the configuration being implemented.

Table 79. IP addressing requirements for exposed hosts in a dual WAN port configuration

Configuration and WAN IP address		**Single WAN port (reference case)**	**Dual WAN port cases**	
			Rollover	**Load Balancing**
Inbound traffic • Port forwarding • Port triggering	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required

Inbound Traffic to a Single WAN Port System

The Internet IP address of the VPN firewall's WAN port needs to be known to the public so that the public can send incoming traffic to the exposed host when this feature is supported and enabled.

In the single WAN case, the WAN's Internet address is either fixed IP or an FQDN if the IP address is dynamic.

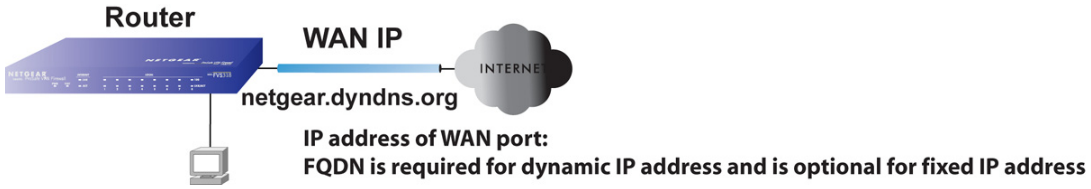

Router
WAN IP
INTERNET
netgear.dyndns.org
IP address of WAN port:
FQDN is required for dynamic IP address and is optional for fixed IP address

Figure 185.

Inbound Traffic to a Dual WAN Port System

The IP address range of the VPN firewall's WAN port needs to be both fixed and public so that the public can send incoming traffic to the multiple exposed hosts when this feature is supported and enabled.

Inbound Traffic: Dual WAN Ports for Improved Reliability

In a dual WAN port auto-rollover configuration, the WAN port's IP address will always change when a rollover occurs. You need to use an FQDN that toggles between the IP addresses of the WAN ports (that is, WAN1 or WAN2).

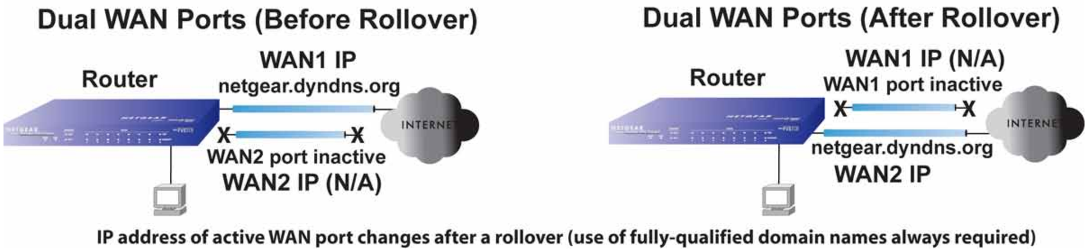
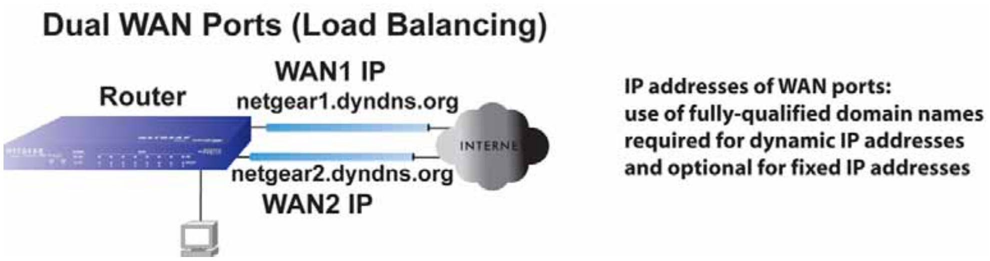

Dual WAN Ports (Before Rollover)
Router
WAN1 IP
netgear.dyndns.org
INTERNET
WAN2 port inactive
WAN2 IP (N/A)
Dual WAN Ports (After Rollover)
Router
WAN1 IP (N/A)
WAN1 port inactive
INTERNET
netgear.dyndns.org
WAN2 IP
IP address of active WAN port changes after a rollover (use of fully-qualified domain names always required)

Figure 186.

Inbound Traffic: Dual WAN Ports for Load Balancing

In a dual WAN port load balancing configuration, the Internet address of each WAN port is either fixed if the IP address is fixed or an FQDN if the IP address is dynamic (see the following figure).

Note: Load balancing is implemented for outgoing traffic and not for incoming traffic. Consider making one of the WAN port Internet addresses public and keeping the other one private in order to maintain better control of WAN port traffic.



IP addresses of WAN ports: use of fully-qualified domain names required for dynamic IP addresses and optional for fixed IP addresses

Figure 187.

Virtual Private Networks

When implementing virtual private network (VPN) tunnels, you need to use a mechanism for determining the IP addresses of the tunnel endpoints. The addressing of the firewall's WAN ports in a dual WAN port auto-rollover or load balancing configuration depends on the configuration being implemented.

Table 80. IP addressing requirements for VPNs in a dual WAN port configuration

Configuration and WAN IP address		**Single WAN port configurations (reference cases)**	**Dual WAN port configurations**	
			Rollover mode[a]	**Load balancing mode**
VPN Road Warrior (Client-to-Gateway)	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required
VPN Gateway-to-Gateway	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required
VPN Telecommuter (Client-to-Gateway through a NAT Router)	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required

[a] *After a rollover, all tunnels need to be reestablished using the new WAN IP address.*

For a single WAN gateway configuration, use ann FQDN when the IP address is dynamic and either an FQDN or the IP address itself when the IP address is fixed. The situation is different in dual WAN port gateway configurations.

- **Dual WAN ports in auto-rollover mode**. A dual WAN port auto-rollover gateway configuration is different from a single WAN port gateway configuration when you specify the IP address of the VPN tunnel endpoint. Only one WAN port is active at a time, and when it rolls over, the IP address of the active WAN port always changes. Therefore, the use of an FQDN is always required, even when the IP address of each WAN port is fixed.

> **Note:** When the VPN firewall's WAN port rolls over, the VPN tunnel collapses and needs to be reestablished using the new WAN IP address. However, you can configure automatic IPSec VPN rollover to ensure that an IPSec VPN tunnel is reestablished.

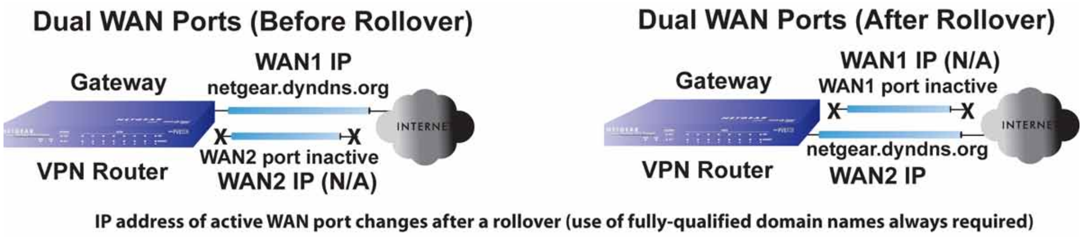

Dual WAN Ports (Before Rollover)
Gateway
WAN1 IP
netgear.dyndns.org
INTERNET
WAN2 port inactive
WAN2 IP (N/A)
VPN Router
Dual WAN Ports (After Rollover)
Gateway
WAN1 IP (N/A)
WAN1 port inactive
INTERNET
netgear.dyndns.org
WAN2 IP
VPN Router
IP address of active WAN port changes after a rollover (use of fully-qualified domain names always required)

Figure 188. f

- **Dual WAN ports in load balancing mode**. A dual WAN port load balancing gateway configuration is the same as a single WAN port configuration when you specify the IP address of the VPN tunnel endpoint. Each IP address is either fixed or dynamic based on the ISP: You need to use FQDNs when the IP address is dynamic, and FQDNs are optional when the IP address is static.

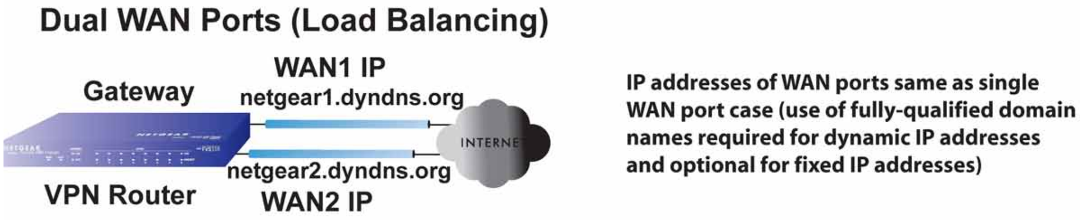

Dual WAN Ports (Load Balancing)
Gateway
WAN1 IP
netgear1.dyndns.org
INTERNET
netgear2.dyndns.org
WAN2 IP
VPN Router
IP addresses of WAN ports same as single WAN port case (use of fully-qualified domain names required for dynamic IP addresses and optional for fixed IP addresses)

Figure 189.

VPN Road Warrior (Client-to-Gateway)

The following situations exemplify the requirements for a remote PC client with no firewall to establish a VPN tunnel with a gateway VPN firewall such as an VPN firewall:

- Single-gateway WAN port
- Redundant dual-gateway WAN ports for increased reliability (before and after rollover)
- Dual-gateway WAN ports for load balancing

VPN Road Warrior: Single Gateway WAN Port (Reference Case)

In a single WAN port gateway configuration, the remote PC client initiates the VPN tunnel because the IP address of the remote PC client is not known in advance. The gateway WAN port needs to act as the responder.

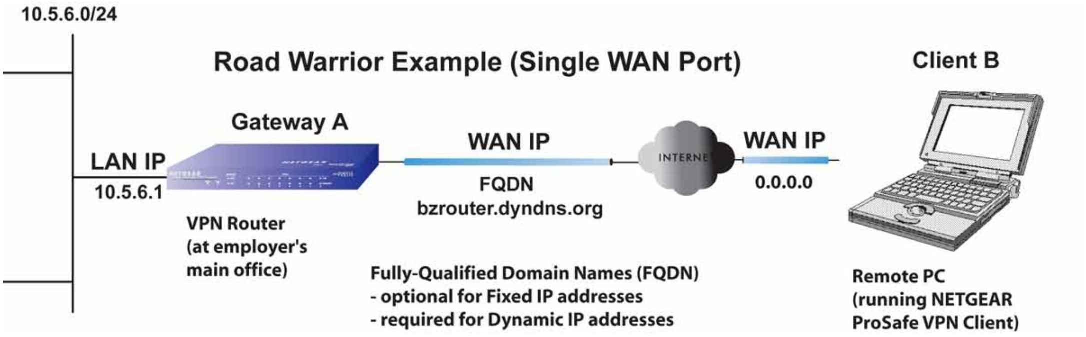


Figure 190.

The IP address of the gateway WAN port can be either fixed or dynamic. If the IP address is dynamic, an FQDN needs to be used. If the IP address is fixed, an FQDN is optional.

VPN Road Warrior: Dual Gateway WAN Ports for Improved Reliability

In a dual WAN port auto-rollover gateway configuration, the remote PC client initiates the VPN tunnel with the active WAN port (port WAN1 in the following figure) because the IP address of the remote PC client is not known in advance. The gateway WAN port needs to act as a responder.

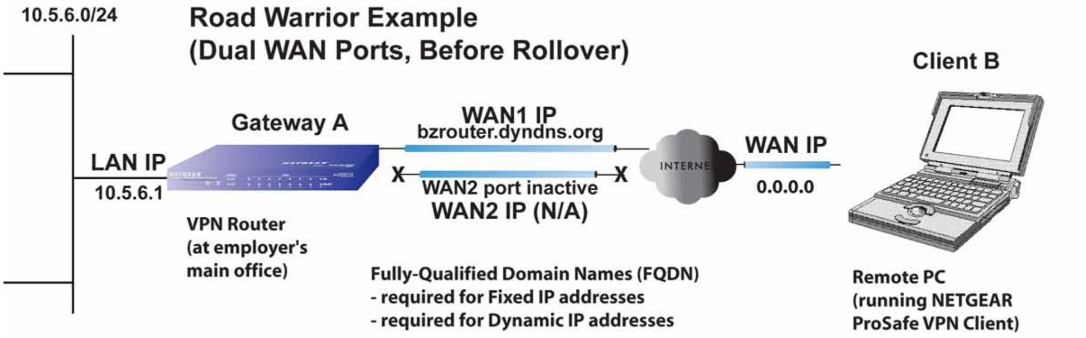


Figure 191.

The IP addresses of the WAN ports can be either fixed or dynamic, but you always need to use an FQDN because the active WAN port could be either WAN1 or WAN2 (that is, the IP address of the active WAN port is not known in advance).

After a rollover of the WAN port has occurred, the previously inactive gateway WAN port becomes the active port (port WAN2 in the following figure) and the remote PC client needs to reestablish the VPN tunnel. The gateway WAN port needs to act as the responder.

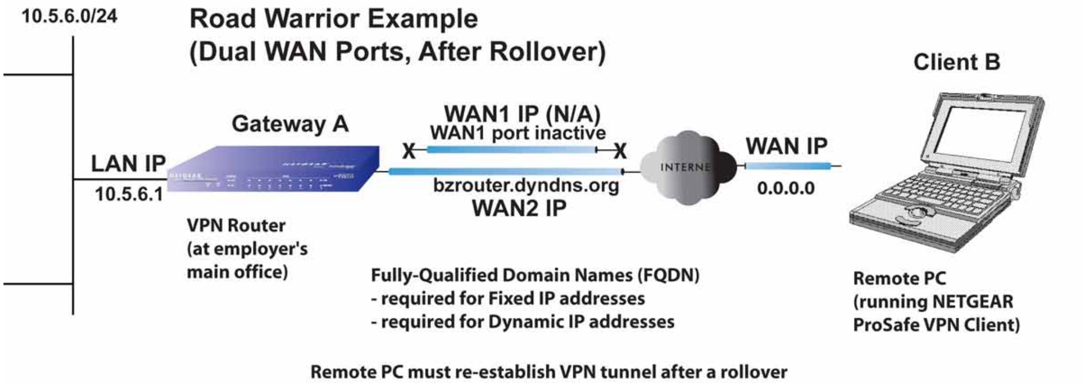


Figure 192.

The purpose of the FQDN in this case is to toggle the domain name of the gateway firewall between the IP addresses of the active WAN port (that is, WAN1 and WAN2) so that the remote PC client can determine the gateway IP address to establish or reestablish a VPN tunnel.

VPN Road Warrior: Dual Gateway WAN Ports for Load Balancing

In a dual WAN port load balancing gateway configuration, the remote PC initiates the VPN tunnel with the appropriate gateway WAN port (that is, port WAN1 or WAN2 as necessary to balance the loads of the two gateway WAN ports) because the IP address of the active WAN port is not known in advance. The selected gateway WAN port needs to act as the responder.

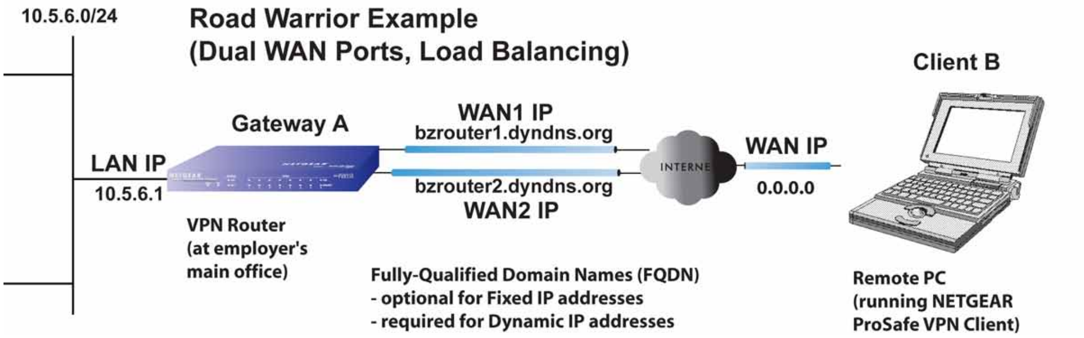


Figure 193.

The IP addresses of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, you need to use an FQDN. If an IP address is fixed, an FQDN is optional.

VPN Gateway-to-Gateway

The following situations exemplify the requirements for a gateway VPN firewall such as an VPN firewall to establish a VPN tunnel with another gateway VPN firewall:

- Single-gateway WAN ports
- Redundant-dual gateway WAN ports for increased reliability (before and after rollover)

- Dual-gateway WAN ports for load balancing

VPN Gateway-to-Gateway: Single Gateway WAN Ports (Reference Case)

In a configuration with two single WAN port gateways, either gateway WAN port can initiate the VPN tunnel with the other gateway WAN port because the IP addresses are known in advance.

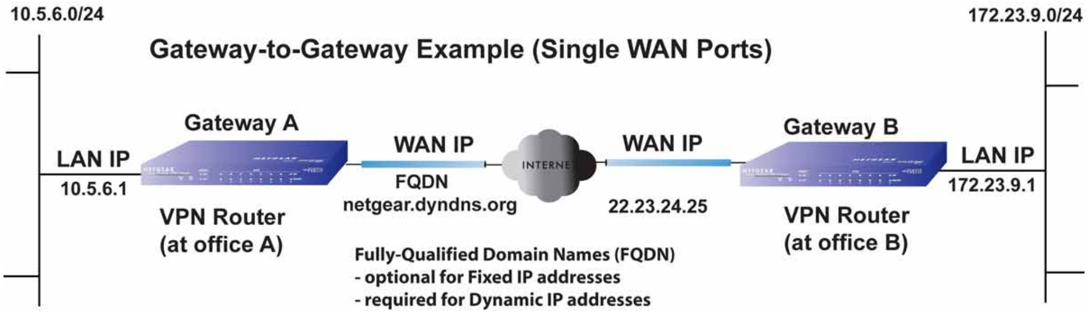


Figure 194.

The IP address of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, you need to use an FQDN. If an IP address is fixed, an FQDN is optional.

VPN Gateway-to-Gateway: Dual Gateway WAN Ports for Improved Reliability

In a configuration with two dual WAN port VPN gateways that function in auto-rollover mode, either of the gateway WAN ports at one end can initiate the VPN tunnel with the appropriate gateway WAN port at the other end as necessary to balance the loads of the gateway WAN ports because the IP addresses of the WAN ports are known in advance. In this example (see the following figure), port WAN_A1 is active and port WAN_A2 is inactive at Gateway A; port WAN_B1 is active and port WAN_B2 is inactive at Gateway B.

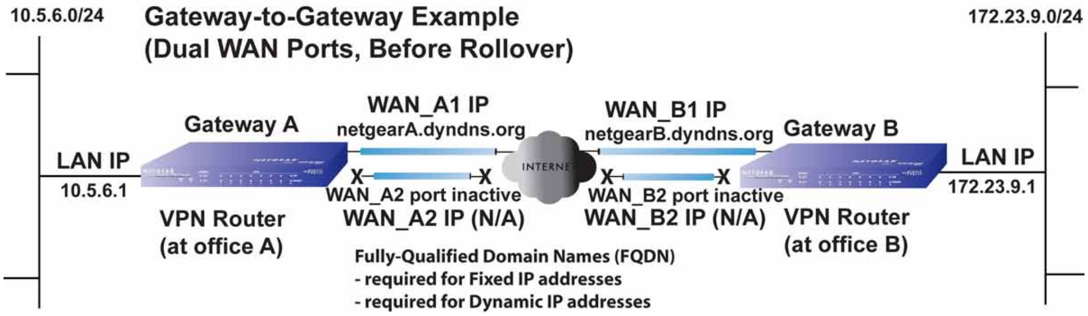


Figure 195.

The IP addresses of the gateway WAN ports can be either fixed or dynamic, but you always need to use an FQDN because the active WAN ports could be either WAN_A1, WAN_A2, WAN_B1, or WAN_B2 (that is, the IP address of the active WAN ports is not known in advance).

After a rollover of a gateway WAN port, the previously inactive gateway WAN port becomes the active port (port WAN_A2 in the following figure), and one of the gateways needs to reestablish the VPN tunnel.

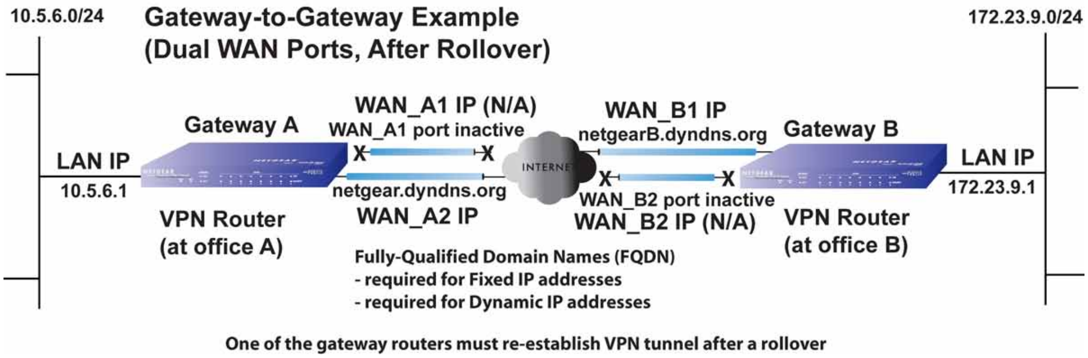


Figure 196.

The purpose of the FQDNs is to toggle the domain name of the rolled-over gateway between the IP addresses of the active WAN port (that is, WAN_A1 and WAN_A2 in the previous figure) so that the other end of the tunnel has a known gateway IP address to establish or reestablish a VPN tunnel.

VPN Gateway-to-Gateway: Dual Gateway WAN Ports for Load Balancing

In a configuration with two dual-WAN port VPN gateways that function in load balancing mode, either of the gateway WAN ports at one end can be programmed in advance to initiate the VPN tunnel with the appropriate gateway WAN port at the other end as necessary to manage the loads of the gateway WAN ports because the IP addresses of the WAN ports are known in advance.

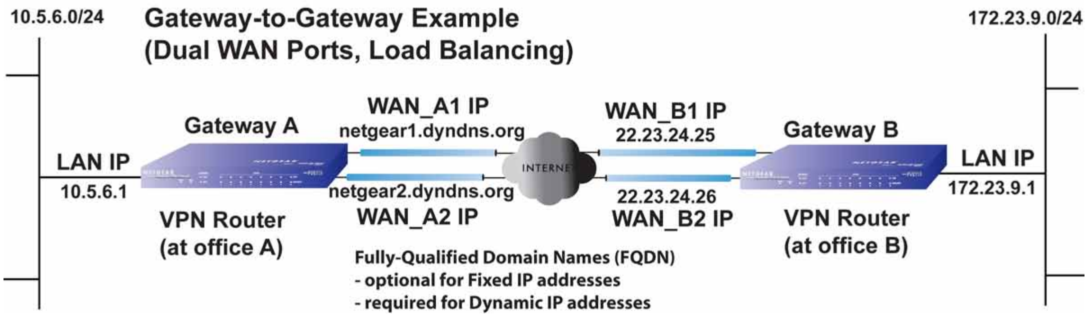


Figure 197.

The IP addresses of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, you need to use an FQDN. If an IP address is fixed, an FQDN is optional.

VPN Telecommuter (Client-to-Gateway through a NAT Router)

Note: The telecommuter case presumes the home office has a dynamic IP address and NAT router.

The following situations exemplify the requirements for a remote PC client connected to the Internet with a dynamic IP address through a NAT router to establish a VPN tunnel with a gateway VPN firewall such as an VPN firewall at the company office:

- Single-gateway WAN port
- Redundant-dual gateway WAN ports for increased reliability (before and after rollover)
- Dual-gateway WAN ports for load balancing

VPN Telecommuter: Single Gateway WAN Port (Reference Case)

In a single WAN port gateway configuration, the remote PC client at the NAT router initiates the VPN tunnel because the IP address of the remote NAT router is not known in advance. The gateway WAN port needs to act as the responder.

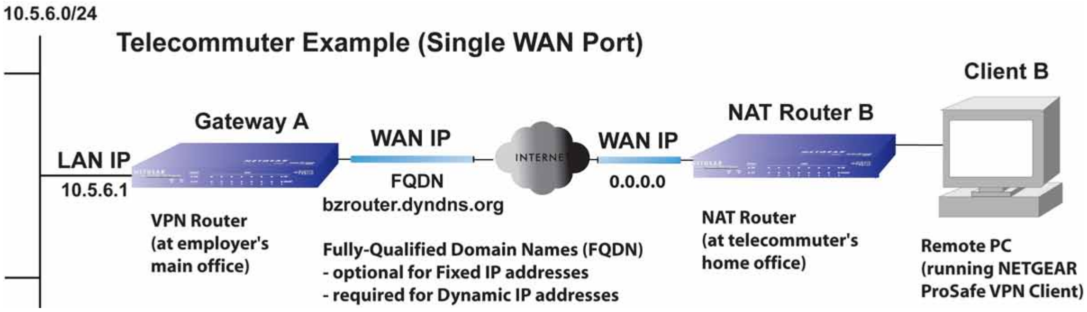


Figure 198.

The IP address of the gateway WAN port can be either fixed or dynamic. If the IP address is dynamic, you need to use an FQDN. If the IP address is fixed, an FQDN is optional.

VPN Telecommuter: Dual Gateway WAN Ports for Improved Reliability

In a dual WAN port auto-rollover gateway configuration, the remote PC client initiates the VPN tunnel with the active gateway WAN port (port WAN1 in the following figure) because the IP address of the remote NAT router is not known in advance. The gateway WAN port needs to act as the responder.

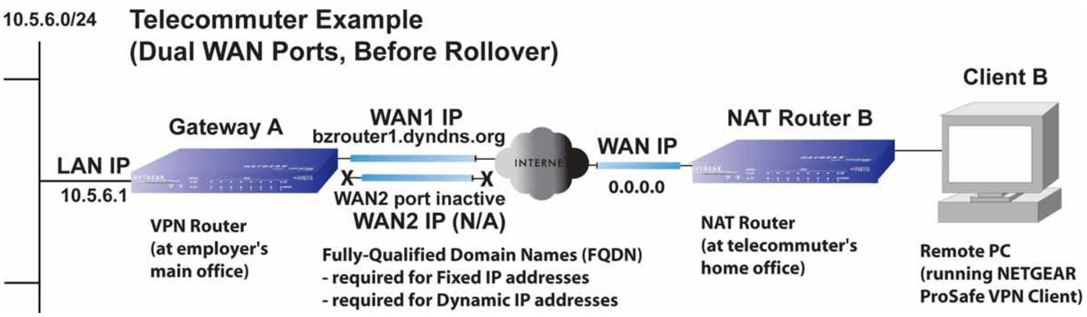


Figure 199.

The IP addresses of the gateway WAN ports can be either fixed or dynamic, but you always need to use an FQDN because the active WAN port could be either WAN1 or WAN2 (that is, the IP address of the active WAN port is not known in advance).

After a rollover of the WAN port has occurred, the previously inactive gateway WAN port becomes the active port (port WAN2 in the following figure) and the remote PC needs to reestablish the VPN tunnel. The gateway WAN port needs to act as the responder.

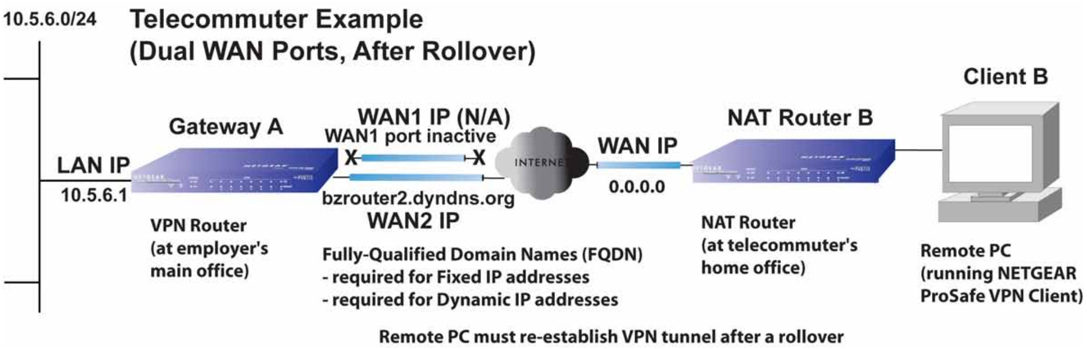


Figure 200.

The purpose of the FQDN is to toggle the domain name of the gateway between the IP addresses of the active WAN port that is, WAN1 and WAN2) so that the remote PC client can determine the gateway IP address to establish or reestablish a VPN tunnel.

VPN Telecommuter: Dual Gateway WAN Ports for Load Balancing

In a dual WAN port load balancing gateway configuration, the remote PC client initiates the VPN tunnel with the appropriate gateway WAN port (that is, port WAN1 or WAN2 as necessary to balance the loads of the two gateway WAN ports) because the IP address of the remote NAT router is not known in advance. The selected gateway WAN port needs to act as the responder.

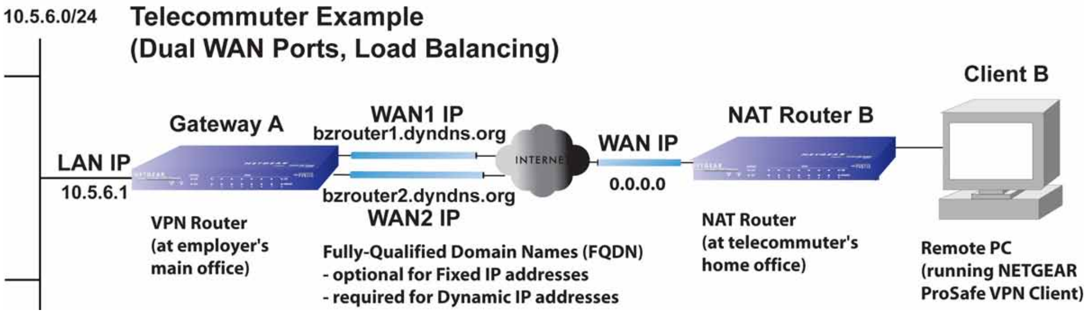


Figure 201.

The IP addresses of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, you need to use an FQDN. If an IP address is fixed, an FQDN is optional.

System Logs and Error Messages

C

This appendix provides examples and explanations of system logs and error message. When applicable, a recommended action is provided.

This appendix contains the following sections:

- *System Log Messages*
- *Routing Logs*
- *Other Event Logs*
- *DHCP Logs*

This appendix uses the following log message terms.

Table 81. Log message terms

Term	Description
[SRX5308]	System identifier.
[kernel]	Message from the kernel.
CODE	Protocol code (e.g., protocol is ICMP, type 8) and CODE=0 means successful reply.
DEST	Destination IP address of the machine to which the packet is destined.
DPT	Destination port.
IN	Incoming interface for packet.
OUT	Outgoing interface for packet.
PROTO	Protocol used.
SELF	Packet coming from the system only.
SPT	Source port.
SRC	Source IP address of machine from which the packet is coming.
TYPE	Protocol type.

System Log Messages

This section describes log messages that belong to one of the following categories:

- Logs generated by traffic that is meant for the VPN firewall.
- Logs generated by traffic that is routed or forwarded through the VPN firewall.
- Logs generated by system daemons; the NTP daemon, the WAN daemon, and others daemons.

To select many of these logs, see *Activate Notification of Events, Alerts, and Syslogs* on page 269.

NTP

This section describes log messages generated by the NTP daemon during synchronization with the NTP server.

Table 82. System logs: NTP

Message	Nov 28 12:31:13 [SRX5308] [ntpdate] Looking Up time-f.netgear.com Nov 28 12:31:13 [SRX5308] [ntpdate] Requesting time from time-f.netgear.com Nov 28 12:31:14 [SRX5308] [ntpdate] adjust time server 69.25.106.19 offset 0.140254 sec Nov 28 12:31:14 [SRX5308] [ntpdate] Synchronized time with time-f.netgear.com Nov 28 12:31:16 [SRX5308] [ntpdate] Date and Time Before Synchronization: Tue Nov 28 12:31:13 GMT+0530 2006 Nov 28 12:31:16 [SRX5308] [ntpdate] Date and Time After Synchronization: Tue Nov 28 12:31:16 GMT+0530 2006 Nov 28 12:31:16 [SRX5308] [ntpdate] Next Synchronization after 2 Hours
Explanation	Message 1: DNS resolution for the NTP server (time-f.netgear.com). Message 2: Request for NTP update from the time server. Message 3: Adjust time by re-setting system time. Message 4: Display date and time before synchronization, that is, when resynchronization started. Message 5: Display the new updated date and time. Message 6: Next synchronization will be after the specified time. Example: In these logs the next synchronization will be after 2 hours. The synchronization time interval is configurable via the CLI.
Recommended Action	None

Login/Logout

This section describes logs generated by the administrative interfaces of the device.

Table 83. System logs: login/logout

Message	Nov 28 14:45:42 [SRX5308] [login] Login succeeded: user admin from 192.168.10.10
Explanation	Login of user admin from host with IP address 192.168.10.10.
Recommended Action	None
Message	Nov 28 14:55:09 [SRX5308] [seclogin] Logout succeeded for user admin Nov 28 14:55:13 [SRX5308] [seclogin] Login succeeded: user admin from 192.168.1.214
Explanation	Secure login/logout of user admin from host with IP address 192.168.1.214.
Recommended Action	None

System Startup

This section describes log messages generated during system startup.

Table 84. System logs: system startup

Message	Jan 1 15:22:28 [SRX5308] [ledTog] [SYSTEM START-UP] System Started
Explanation	Log generated when the system is started.
Recommended Action	None

Reboot

This section describes log messages generated during system reboot.

Table 85. System logs: reboot

Message	Nov 25 19:42:57 [SRX5308] [reboot] Rebooting in 3 seconds
Explanation	Log generated when the system is rebooted from the web management interface.
Recommended Action	None

Firewall Restart

This section describes logs that are generated when the VPN firewall restarts.

Table 86. System logs: VPN firewall restart

Message	Jan 23 16:20:44 [SRX5308] [wand] [FW] Firewall Restarted
Explanation	Log generated when the VPN firewall is restarted. This message is logged when the VPN firewall restarts after any changes in the configuration are applied.
Recommended Action	None

IPSec Restart

This section describes logs that are generated when IPSec restarts.

Table 87. System logs: IPSec restart

Message	Jan 23 16:20:44 [SRX5308] [wand] [IPSEC] IPSEC Restarted
Explanation	Log generated when the IPSec is restarted. This message is logged when IPSec restarts after any changes in the configuration are applied.
Recommended Action	None

Unicast, Multicast, and Broadcast Logs

Table 88. System logs: unicast

Message	Nov 24 11:52:55 [SRX5308] [kernel] UCAST IN=SELF OUT=WAN SRC= 192.168.10.1 DST=192.168.10.10 PROTO=UDP SPT=800 DPT=2049
Explanation	• This packet (unicast) is sent to the device from the WAN network. • For other settings, see *Table 81* on page 322.
Recommended Action	None

ICMP Redirect Logs

Table 89. System logs: unicast, redirect

Message	Feb 2007 22 14:36:07 [SRX5308] [kernel] [LOG_PACKET] SRC=192.168.1.49 DST=192.168.1.124 PROTO=ICMP TYPE=5 CODE=1
Explanation	• This packet is an ICMP redirect message sent to the device by another device. • For other settings, see *Table 81* on page 322.

Recommended Action	To enable these logs, from the CLI command prompt of the VPN firewall, enter this command:
	`monitor/firewallLogs/logger/loggerConfig logIcmpRedirect 1`
	And to disable it enter:
	`monitor/firewallLogs/logger/loggerConfig logIcmpRedirect 0`

Multicast/Broadcast Logs

Table 90. System logs: multicast/broadcast

Message	Jan 1 07:24:13 [SRX5308] [kernel] MCAST-BCAST IN=WAN OUT=SELF SRC= 192.168.1.73 DST=192.168.1.255 PROTO=UDP SPT=138 DPT=138
Explanation	• This multicast or broadcast packet is sent to the device from the WAN network. • For other settings, see *Table 81* on page 322.
Recommended Action	None

WAN Status

This section describes the logs generated by the WAN component. If there are several ISP links for Internet connectivity, the VPN firewall can be configured either in auto-rollover or load balancing mode.

Load Balancing

When the WAN mode is configured for load balancing, all the WAN ports are active simultaneously and the traffic is balanced between them. If one WAN link goes down, all the traffic is diverted to the other WAN links that are active.

This section describes the logs generated when the WAN mode is set to load balancing.

Table 91. System logs: WAN status, load balancing

Message	Dec 1 12:11:27 [SRX5308] [wand] [LBFO] Restarting WAN1_ Dec 1 12:11:31 [SRX5308] [wand] [LBFO] Restarting WAN2_ Dec 1 12:11:35 [SRX5308] [wand] [LBFO] WAN1(UP), WAN2(UP)_ Dec 1 12:24:12 [SRX5308] [wand] [LBFO] WAN1(UP), WAN2(DOWN)_ Dec 1 12:29:43 [SRX5308] [wand] [LBFO] Restarting WAN2_ Dec 1 12:29:47 [SRX5308] [wand] [LBFO] WAN1(UP), WAN2(DOWN)_
Explanation	Message 1 and Message 2 indicate that both the WANs are restarted. Message 3: This message shows that both the WANs are up and the traffic is balanced between the two WAN interfaces. Message 4: This message shows that one of the WAN links is down. At this point, all the traffic is directed through the WAN that is up.
Recommended Action	None

Auto-Rollover

When the WAN mode is configured for auto-rollover, the primary link is active and the secondary link acts only as a backup. When the primary link goes down, the secondary link becomes active only until the primary link comes back up. The VPN firewall monitors the status of the primary link using the configured WAN failure detection method.

This section describes the logs generated when the WAN mode is set to auto-rollover.

Table 92. System logs: WAN status, auto-rollover

Message	Nov 17 09:59:09 [SRX5308] [wand] [LBFO] WAN1 Test Failed 1 of 3 times_ Nov 17 09:59:39 [SRX5308] [wand] [LBFO] WAN1 Test Failed 2 of 3 times_ Nov 17 10:00:09 [SRX5308] [wand] [LBFO] WAN1 Test Failed 3 of 3 times_ Nov 17 10:01:01 [SRX5308] [wand] [LBFO] WAN1 Test Failed 4 of 3 times_ Nov 17 10:01:35 [SRX5308] [wand] [LBFO] WAN1 Test Failed 5 of 3 times_ Nov 17 10:01:35 [SRX5308] [wand] [LBFO] WAN1(DOWN), WAN2(UP), ACTIVE(WAN2)_ Nov 17 10:02:25 [SRX5308] [wand] [LBFO] WAN1 Test Failed 6 of 3 times_ Nov 17 10:02:25 [SRX5308] [wand] [LBFO] Restarting WAN1_ Nov 17 10:02:57 [SRX5308] [wand] [LBFO] WAN1 Test Failed 7 of 3 times_ Nov 17 10:03:27 [SRX5308] [wand] [LBFO] WAN1 Test Failed 8 of 3 times_ Nov 17 10:03:57 [SRX5308] [wand] [LBFO] WAN1 Test Failed 9 of 3 times_ Nov 17 10:03:57 [SRX5308] [wand] [LBFO] Restarting WAN1_

Table 92. System logs: WAN status, auto-rollover (continued)

Explanation	The logs suggest that the failover was detected after 5 attempts instead of 3. However, the reason that the messages appear in the log is because of the WAN state transition logic, which is part of the failover algorithm. These logs can be interpreted as follows: The primary link failure is correctly detected after the 3rd attempt. Thereafter, the algorithm attempts to restart the WAN connection and checks once again to determine if WAN1 is still down. This results in the 4th failure detection message. If it is still down, then it starts a secondary link, and once the secondary link is up, the secondary link is marked as active. Meanwhile, the primary link has failed once more, and that results in the 5th failure detection message. Note that the 5th failure detection message and the message suggesting that the secondary link is active have the same timestamp, and so they happen in the same algorithm state–machine cycle. So although it appears that the failover did not happen immediately after 3 failures, internally, the failover process is triggered after the 3rd failure, and transition to the secondary link is completed by the 5th failure. The primary link is also restarted every 3 failures till it is functional again. In these logs, the primary link was restarted after the 6th failure, that is, 3 failures after the failover process was triggered.
Recommended Action	Check the WAN settings and WAN failure detection method configured for the primary link.

PPP Logs

This section describes the WAN PPP connection logs. The PPP type can be configured from the web management interface (see *Manually Configure the Internet Connection* on page 28).

- PPPoE Idle Timeout Logs

Table 93. System logs: WAN status, PPPoE idle time-out

Message	Nov 29 13:12:46 [SRX5308] [pppd] Starting connection Nov 29 13:12:49 [SRX5308] [pppd] Remote message: Success Nov 29 13:12:49 [SRX5308] [pppd] PAP authentication succeeded Nov 29 13:12:49 [SRX5308] [pppd] local IP address 50.0.0.62 Nov 29 13:12:49 [SRX5308] [pppd] remote IP address 50.0.0.1 Nov 29 13:12:49 [SRX5308] [pppd] primary DNS address 202.153.32.3 Nov 29 13:12:49 [SRX5308] [pppd] secondary DNS address 202.153.32.3 Nov 29 11:29:26 [SRX5308] [pppd] Terminating connection due to lack of activity. Nov 29 11:29:28 [SRX5308] [pppd] Connect time 8.2 minutes. Nov 29 11:29:28 [SRX5308] [pppd] Sent 1408 bytes, received 0 bytes. Nov 29 11:29:29 [SRX5308] [pppd] Connection terminated.

Table 93. System logs: WAN status, PPPoE idle time-out (continued)

Explanation	Message 1: PPPoE connection started. Message 2: Message from PPPoE server for correct login. Message 3: Authentication for PPP succeeded. Message 4: Local IP address assigned by the server. Message 5: Server side IP address. Message 6: The primary DNS server that is configured on the WAN ISP Settings screen. Message 7: The secondary DNS server that is configured on the WAN ISP Settings screen. Message 8: The PPP link has transitioned to idle mode. This event occurs if there is no traffic from the LAN network. Message 9: The time in minutes for which the link has been up. Message 10: Data sent and received at the LAN side while the link was up. Message 11: PPP connection terminated after idle timeout.
Recommended Action	To reconnect during idle mode, initiate traffic from the LAN side.

- PPTP Idle Timeout Logs

Table 94. System logs: WAN status, PPTP idle time-out

Message	Nov 29 11:19:02 [SRX5308] [pppd] Starting connection Nov 29 11:19:05 [SRX5308] [pppd] CHAP authentication succeeded Nov 29 11:19:05 [SRX5308] [pppd] local IP address 192.168.200.214 Nov 29 11:19:05 [SRX5308] [pppd] remote IP address 192.168.200.1 Nov 29 11:19:05 [SRX5308] [pppd] primary DNS address 202.153.32.2 Nov 29 11:19:05 [SRX5308] [pppd] secondary DNS address 202.153.32.2 Nov 29 11:20:45 [SRX5308] [pppd] No response to 10 echo-requests Nov 29 11:20:45 [SRX5308] [pppd] Serial link appears to be disconnected. Nov 29 11:20:45 [SRX5308] [pppd] Connect time 1.7 minutes. Nov 29 11:20:45 [SRX5308] [pppd] Sent 520 bytes, received 80 bytes. Nov 29 11:20:51 [SRX5308] [pppd] Connection terminated.
Explanation	Message 1: Starting PPP connection process. Message 2: Message from the server for authentication success. Message 3: Local IP address assigned by the server. Message 4: Server side IP address. Message 6: The primary DNS server that is configured on the WAN ISP Settings screen. Message 7: The secondary DNS server that is configured on the WAN ISP Settings screen. Message 7: Sensing idle link. Message 8: Idle link sensed. Message 9: Data sent and received at the LAN side while the link was up. Message 10: PPP connection terminated after idle timeout.
Recommended Action	To reconnect during idle mode, initiate traffic from the LAN side.

- PPP Authentication Logs

Table 95. System logs: WAN status, PPP authentication

Message	Nov 29 11:29:26 [SRX5308] [pppd] Starting link Nov 29 11:29:29 [SRX5308] [pppd] Remote message: Login incorrect Nov 29 11:29:29 [SRX5308] [pppd] PAP authentication failed Nov 29 11:29:29 [SRX5308] [pppd] Connection terminated.WAN2(DOWN)_
Explanation	Starting link: Starting PPPoE connection process. Remote message: Login incorrect: Message from PPPoE server for incorrect login. PAP authentication failed: PPP authentication failed due to incorrect login. Connection terminated: PPP connection terminated.
Recommended Action	If authentication fails, then check the login/password and enter the correct one.

Resolved DNS Names

This section describes the logs of DNS names resolution messages.

Table 96. System logs: DNS names resolution messages

Message	2000 Jan 1 05:12:00 [SRX5308] [dnsmasq] [DNSRESOLV]:teamf1.com from 192.168.11.2
Explanation	This log is generated when the DNS name (that is, teamf1) is resolved.
Recommended Action	None

VPN Log Messages

This section explains logs that are generated by IPSec VPN and SSL VPN policies. These logs are generated automatically and do not need to be enabled.

IPSec VPN Logs

This section describes the log messages generated by IPSec VPN policies.

Note: The same IPSec VPN log messages can appear in the logs that are accessible when you select the **VPN** check box on the Firewall Logs & E-mail screen (see *Activate Notification of Events, Alerts, and Syslogs* on page 269) and in the logs on the IPSec VPN Logs screen (see *View the VPN Logs* on page 283).

Table 97. System logs: IPSec VPN tunnel, tunnel establishment

Messages 1 through 5	2000 Jan 1 04:01:39 [SRX5308] [wand] [IPSEC] IPSEC Restarted
	2000 Jan 1 04:02:09 [SRX5308] [wand] [FW] Firewall Restarted
	2000 Jan 1 04:02:29 [SRX5308] [IKE] IKE stopped_
	2000 Jan 1 04:02:31 [SRX5308] [IKE] IKE started_
	2000 Jan 1 04:02:31 [SRX5308] [wand] [IPSEC] IPSEC Restarted
Messages 6 and 7	2000 Jan 1 04:07:04 [SRX5308] [IKE] Adding IPSec configuration with identifier "pol1"_
	2000 Jan 1 04:07:04 [SRX5308] [IKE] Adding IKE configuration with identifier "pol1"_
Messages 8 through 19	2000 Jan 1 04:13:39 [SRX5308] [IKE] Configuration found for 20.0.0.1[500]._
	2000 Jan 1 04:13:39 [SRX5308] [IKE] Received request for new phase 1 negotiation: 20.0.0.2[500]<=>20.0.0.1[500]_
	2000 Jan 1 04:13:39 [SRX5308] [IKE] Beginning Identity Protection mode._
	2000 Jan 1 04:13:39 [SRX5308] [IKE] Received Vendor ID: RFC XXXX_
	2000 Jan 1 04:13:39 [SRX5308] [IKE] Received Vendor ID: DPD_
	2000 Jan 1 04:13:39 [SRX5308] [IKE] DPD is Enabled_
	2000 Jan 1 04:13:39 [SRX5308] [IKE] For 20.0.0.1[500], Selected NAT-T version: RFC XXXX_
	2000 Jan 1 04:13:39 [SRX5308] [IKE] Setting DPD Vendor ID_
	2000 Jan 1 04:13:39 [SRX5308] [IKE] Received Vendor ID: KAME/racoon_
	2000 Jan 1 04:13:39 [SRX5308] [IKE] NAT-D payload matches for 20.0.0.2[500]_
	2000 Jan 1 04:13:39 [SRX5308] [IKE] NAT-D payload matches for 20.0.0.1[500]_
	2000 Jan 1 04:13:39 [SRX5308] [IKE] NAT not detected _
Messages 20 and 21	2000 Jan 1 04:13:39 [SRX5308] [IKE] ISAKMP-SA established for 20.0.0.2[500]-20.0.0.1[500] with spi:c56f7a1d42baf28a:68fcf85e3c148bd8_
	2000 Jan 1 04:13:39 [SRX5308] [IKE] Sending Informational Exchange: notify payload[INITIAL-CONTACT]_
Messages 22 and 23	2000 Jan 1 04:13:40 [SRX5308] [IKE] Responding to new phase 2 negotiation: 20.0.0.2[0]<=>20.0.0.1[0]_
	2000 Jan 1 04:13:40 [SRX5308] [IKE] Using IPSec SA configuration: 192.168.11.0/24<->192.168.10.0/24_
Messages 24 and 25	2000 Jan 1 04:13:41 [SRX5308] [IKE] IPSec-SA established: ESP/Tunnel 20.0.0.1->20.0.0.2 with spi=34046092(0x207808c)_
	2000 Jan 1 04:13:41 [SRX5308] [IKE] IPSec-SA established: ESP/Tunnel 20.0.0.2->20.0.0.1 with spi=87179451(0x53240bb)_
Explanation	Message 1–5: IPSec, IKE, and VPN firewall restart. Message 6–7: IPSec and IKE configurations are added with the identifier “pol1.” Message 8–19: New phase 1 negotiation starts by determining the configuration for the WAN host. Dead Peer Detection (DPD) is enabled and set. NAT payload matching and NAT detection are done. Message 20–21: ISAKMP-SA is established between the 2 WANs and information is exchanged. Message 22–23: New phase 2 negotiation starts by using IPSec SA configuration pertaining to the LAN hosts. Message 24–25: IPSec-SA VPN tunnel is established.
Recommended Action	None

Table 98. System logs: IPSec VPN tunnel, SA lifetime (150 sec in phase 1; 300 sec in phase 2), VPN tunnel is reestablished

Message 1	2000 Jan 1 04:32:25 [SRX5308] [IKE] Sending Informational Exchange: delete payload[]_
Messages 2 through 6	2000 Jan 1 04:32:25 [SRX5308] [IKE] purged IPSec-SA proto_id=ESP spi= 181708762._
	2000 Jan 1 04:32:25 [SRX5308] [IKE] purged IPSec-SA proto_id=ESP spi= 153677140._
	2000 Jan 1 04:32:25 [SRX5308] [IKE] an undead schedule has been deleted: 'pk_recvupdate'._
	2000 Jan 1 04:32:25 [SRX5308] [IKE] IPSec configuration with identifier "pol1" deleted successfully_
	2000 Jan 1 04:32:25 [SRX5308] [IKE] no phase 2 bounded._
Message 7	2000 Jan 1 04:32:25 [SRX5308] [IKE] Sending Informational Exchange: delete payload[]_
Messages 8 through 11	2000 Jan 1 04:32:25 [SRX5308] [IKE] Purged ISAKMP-SA with spi= d67f2be9ca0cb241:8a094623c6811286._
	2000 Jan 1 04:32:25 [SRX5308] [IKE] an undead schedule has been deleted: 'purge_remote'._
	2000 Jan 1 04:32:25 [SRX5308] [IKE] IKE configuration with identifier "pol1" deleted successfully_
	2000 Jan 1 04:32:25 [SRX5308] [IKE] Could not find configuration for 20.0.0.1[500]_
Explanation	Message 1: Informational exchange for deleting the payload. Message 2–6: Phase 2 configuration is purged and confirms that no phase 2 is bounded. Message 7: Informational exchange for deleting the payload. Message 8–11: Phase 1 configuration. The VPN tunnel is reestablished.
Recommended Action	None

Table 99. System logs: IPSec VPN tunnel, SA lifetime (150 sec in phase 1; 300 sec in phase 2), VPN tunnel not reestablished

Message	2000 Jan 1 04:52:33 [SRX5308] [IKE] Using IPSec SA configuration: 192.168.11.0/24<->192.168.10.0/24_ 2000 Jan 1 04:52:33 [SRX5308] [IKE] Configuration found for 20.0.0.1._ 2000 Jan 1 04:52:59 [SRX5308] [IKE] Phase 1 negotiation failed due to time up for 20.0.0.1[500]. b73efd188399b7f2:0000000000000000_ 2000 Jan 1 04:53:04 [SRX5308] [IKE] Phase 2 negotiation failed due to time up waiting for phase 1. ESP 20.0.0.1->20.0.0.2 _ 2000 Jan 1 04:53:05 [SRX5308] [IKE] Using IPSec SA configuration: 192.168.11.0/24<->192.168.10.0/24_ 2000 Jan 1 04:53:05 [SRX5308] [IKE] Configuration found for 20.0.0.1._ 2000 Jan 1 04:53:05 [SRX5308] [IKE] Initiating new phase 1 negotiation: 20.0.0.2[500]<=>20.0.0.1[500]_ 2000 Jan 1 04:53:05 [SRX5308] [IKE] Beginning Identity Protection mode._ 2000 Jan 1 04:53:05 [SRX5308] [IKE] Setting DPD Vendor ID_ 2000 Jan 1 04:53:36 [SRX5308] [IKE] Phase 2 negotiation failed due to time up waiting for phase 1. ESP 20.0.0.1->20.0.0.2 _
Explanation	Phase 1 and phase 2 negotiations failed because of a mismatch of the WAN IP address in the IPSec VPN policy and the WAN IP address of the remote host attempting to establish the IPSec VPN tunnel.
Recommended Action	None

Table 100. System logs: IPSec VPN tunnel, Dead Peer Detection and keep-alive (default 30 sec)

Messages 1 through 4	2000 Jan 1 04:13:39 [SRX5308] [IKE] Received request for new phase 1 negotiation: 20.0.0.2[500]<=>20.0.0.1[500]_ 2000 Jan 1 04:13:39 [SRX5308] [IKE] Beginning Identity Protection mode._ 2000 Jan 1 04:13:39 [SRX5308] [IKE] Received Vendor ID: RFC XXXX_ 2000 Jan 1 04:13:39 [SRX5308] [IKE] Received Vendor ID: DPD_
Message 5	2000 Jan 1 04:13:39 [SRX5308] [IKE] DPD is Enabled_
Message 6	2000 Jan 1 04:13:39 [SRX5308] [IKE] For 20.0.0.1[500], Selected NAT-T version: RFC XXXX_
Message 7	2000 Jan 1 04:13:39 [SRX5308] [IKE] Setting DPD Vendor ID_
Explanation	Message 1–4: After receiving a request for phase 1 negotiation, a Dead Peer Detection Vendor ID is received. Message 5: DPD is enabled. Message 7: The DPD vendor ID is set.
Recommended Action	None

Table 101. System logs: IPSec VPN tunnel, Dead Peer Detection and keep-alive (default 30 sec), VPN tunnel torn down

Message 1 Message 2 Message 3	2000 Jan 1 06:01:18 [SRX5308] [VPNKA] Keep alive to peer 192.168.10.2 failed 3 consecutive times and 5 times cumulative_ 2000 Jan 1 06:01:19 [SRX5308] [IKE] DPD R-U-THERE sent to "20.0.0.1[500]"_ 2000 Jan 1 06:01:19 [SRX5308] [IKE] DPD R-U-THERE-ACK received from "20.0.0.1[500]"_
Explanation	Message 1: When the remote host connection is removed and when there are no packets from the remote host, the VPN firewall sends packets to keep the remote host alive. As the connection itself is removed, keep-alive fails. Message 2: The VPN firewall sends packets to check whether the peer is dead. Message 3: The VPN firewall receives an acknowledgment that the peer is dead. The connection is removed.
Recommended Action	None

Table 102. System logs: IPSec VPN tunnel, client policy, disconnection from the client side

Message	2000 Jan 1 02:34:45 [SRX5308] [IKE] Deleting generated policy for 20.0.0.1[0]_ 2000 Jan 1 02:34:45 [SRX5308] [IKE] an undead schedule has been deleted: 'pk_recvupdate'._ 2000 Jan 1 02:34:45 [SRX5308] [IKE] Purged IPSec-SA with proto_id=ESP and spi=3000608295(0xb2d9a627)._ 2000 Jan 1 02:34:45 [SRX5308] [IKE] Purged IPSec-SA with proto_id=ESP and spi=248146076(0xeca689c)._ 2000 Jan 1 02:34:45 [SRX5308] [IKE] Purged ISAKMP-SA with proto_id=ISAKMP and spi=da1f2efbf0635943:4eb6fae677b2e4f4._ 2000 Jan 1 02:34:46 [SRX5308] [IKE] ISAKMP-SA deleted for 20.0.0.2[500]-20.0.0.1[500] with spi:da1f2efbf0635943:4eb6fae677b2e4f4_
Explanation	Phase 2 and phase 1 policies are deleted when the client is disconnected.
Recommended Action	None

Table 103. System logs: IPSec VPN tunnel, client policy behind a NAT device

  Message 3 Message 6	2000 Jan 1 01:54:21 [SRX5308] [IKE] Floating ports for NAT-T with peer 20.0.0.1[4500]_ 2000 Jan 1 01:54:21 [SRX5308] [IKE] NAT-D payload matches for 20.0.0.2[4500]_ 2000 Jan 1 01:54:21 [SRX5308] [IKE] NAT-D payload does not match for 20.0.0.1[4500]_ 2000 Jan 1 01:54:21 [SRX5308] [IKE] Ignore REPLAY-STATUS notification from 20.0.0.1[4500]._ 2000 Jan 1 01:54:21 [SRX5308] [IKE] Ignore INITIAL-CONTACT notification from 20.0.0.1[4500] because it is only accepted after phase 1._ 2000 Jan 1 01:54:21 [SRX5308] [IKE] NAT detected: Peer is behind a NAT device_
Explanation	These logs are generated when the remote WAN host is connected through a device such as the VPN firewall. NAT is detected before phase 1 is established. Message 3: NAT-D does not match the remote host. Message 6: The VPN firewall confirms that the remote host or the peer is behind a NAT device.
Recommended Action	None

SSL VPN Logs

This section describes the log messages that are generated by SSL VPN policies.

Table 104. System logs: SSL VPN tunnel, WAN host and interface

Message	2000 Jan 1 03:44:55 [SRX5308] [sslvpntunnel] id=SRX5308 time="2000-1-1 3:44:55" fw=20.0.0.2 pri=6 rule=access-policy proto= "SSL VPN Tunnel" src=20.0.0.1 user=sai dst=20.0.0.2 arg="" op="" result="" rcvd= "" msg="SSL VPN Tunnel"
Explanation	A SSL VPN tunnel is established for ID SRX5308 with the WAN host 20.0.0.1 through WAN interface 20.0.0.2 and logged in with the username “sai.”
Recommended Action	None

Table 105. System logs: VPN log messages, port forwarding, WAN host and interface

Message	2000 Jan 1 01:30:08 [SRX5308] [portforwarding] id=SRX5308 time="2000-1-1 1:30: 8" fw=20.0.0.2 pri=6 rule=access-policy proto= "Port Forwarding" src=20.0.0.1 user=sai dst=20.0.0.2 arg="" op="" result="" rcvd="" msg="Port Forwarding"
Explanation	A SSL VPN tunnel through port forwarding is established for ID SRX5308 with the WAN host 20.0.0.1 through WAN interface 20.0.0.2 and logged in with the username “sai.”
Recommended Action	None

Table 106. System logs: VPN log messages, port forwarding, LAN host and interface

Message	2000 Jan 1 01:35:41 [SRX5308] [portforwarding] id=SRX5308 time="2000-1-1 1:35:41" fw=192.168.11.1 pri=6 rule=access-policy proto="Virtual Transport (Java)" src=192.168.11.2 user=sai dst=192.168.11.1 arg= "" op="" result="" rcvd="" msg="Virtual Transport (Java)"
Explanation	A SSL VPN tunnel through port forwarding is established for ID SRX5308 from the LAN host 192.168.11.2 with interface 192.168.11.1 and logged in with the username “sai.”
Recommended Action	None

Traffic Meter Logs

Table 107. System logs: traffic meter

Message	Jan 23 19:03:44 [TRAFFIC_METER] TRAFFIC_METER: Monthly Limit of 10 MB has reached for WAN1._
Explanation	Traffic limit to WAN1 that was set as 10 Mb has been reached. This stops all the incoming and outgoing traffic, that is, if you selected the **Block All Traffic** radio button in the When Limit is Reached section on the WAN TrafficMeter screen.
Recommended Action	To start the traffic, restart the traffic limit counter.

Routing Logs

This section explains the logging messages for the various network segments (such as LAN to WAN) for debugging purposes. These logs might generate a significant volume of messages.

LAN to WAN Logs

Table 108. Routing Logs: LAN to WAN

Message	Nov 29 09:19:43 [SRX5308] [kernel] LAN2WAN[ACCEPT] IN=LAN OUT=WAN SRC=192.168.10.10 DST=72.14.207.99 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from LAN to WAN has been allowed by the firewall. • For other settings, see *Table 81* on page 322.
Recommended Action	None

LAN to DMZ Logs

Table 109. Routing Logs: LAN to DMZ

Message	Nov 29 09:44:06 [SRX5308] [kernel] LAN2DMZ[ACCEPT] IN=LAN OUT=DMZ SRC=192.168.10.10 DST=192.168.20.10 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from LAN to DMZ has been allowed by the firewall. • For other settings, see *Table 81* on page 322.
Recommended Action	None

DMZ to WAN Logs

Table 110. Routing Logs: DMZ to WAN

Message	Nov 29 09:19:43 [SRX5308] [kernel] DMZ2WAN[DROP] IN=DMZ OUT=WAN SRC=192.168.20.10 DST=72.14.207.99 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from DMZ to WAN has been dropped by the firewall. • For other settings, see *Table 81* on page 322.
Recommended Action	None

WAN to LAN Logs

Table 111. Routing Logs: WAN to LAN

Message	Nov 29 10:05:15 [SRX5308] [kernel] WAN2LAN[ACCEPT] IN=WAN OUT=LAN SRC=192.168.1.214 DST=192.168.10.10 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from LAN to WAN has been allowed by the firewall. • For other settings, see *Table 81* on page 322.
Recommended Action	None

DMZ to LAN Logs

Table 112. Routing Logs: DMZ to WAN

Message	Nov 29 09:44:06 [SRX5308] [kernel] DMZ2LAN[DROP] IN=DMZ OUT=LAN SRC= 192.168.20.10 DST=192.168.10.10 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from DMZ to LAN has been dropped by the firewall. • For other settings, see *Table 81* on page 322.
Recommended Action	None

WAN to DMZ Logs

Table 113. Routing Logs: WAN to DMZ

Message	Nov 29 09:19:43 [SRX5308] [kernel] WAN2DMZ[ACCEPT] IN=WAN OUT=DMZ SRC=192.168.1.214 DST=192.168.20.10 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from WAN to DMZ has been allowed by the firewall. • For other settings, see *Table 81* on page 322.
Recommended Action	None

Other Event Logs

This section describes the log messages generated by other events such source MAC filtering, session limiting, and bandwidth limiting. For information about how to select these logs, see *Activate Notification of Events, Alerts, and Syslogs* on page 269.

Session Limit Logs

Table 114. Other Event Logs: Session Limit Logs

Message	2000 Jan 1 06:53:33 [SRX5308] [kernel] SESS_LIMIT[DROP] IN=LAN OUT=WAN SRC=192.168.11.2 DST=20.0.0.1 PROTO=TCP SPT=50709 DPT=21
Explanation	When two FTP sessions are established from the same LAN host at IP address 192.168.11.2 and a session limit (SESS_LIMIT) is set as 1, the FTP packets from the second session are dropped.
Recommended Action	Change the session limit to 2 to prevent packets from being dropped.

Source MAC Filter Logs

Table 115. Other Event Logs: Source MAC Filter Logs

Message	2000 Jan 1 06:40:10 [SRX5308] [kernel] SRC_MAC_MATCH[DROP] SRC MAC = 00:12:3f:34:41:14 IN=LAN OUT=WAN SRC=192.168.11.3 DST=209.85.153.103 PROTO=ICMP TYPE=8 CODE=0
Explanation	Because MAC address 00:12:3f:34:41:14 of LAN host with IP address 192.168.11.3 is filtered so that it cannot access the Internet, the packets sent by this MAC address to the Google server at address 09.85.153.103 are dropped.
Recommended Action	Disable source MAC filtering.

Bandwidth Limit Logs

Table 116. Other Event Logs: Bandwidth Limit, Outbound Bandwidth Profile

Message	2000 Jan 1 00:10:36 [SRX5308] [kernel] [BW_LIMIT_DROP] IN=LAN OUT=WAN SRC=192.168.100.2 DST=22.0.0.2 PROTO=ICMP TYPE=144 CODE=145 TC_INDEX=10 CLASSID=10:5
Explanation	This log is generated when an outbound packet is dropped because the packet size exceeds the specified bandwidth limit.
Recommended Action	Ensure that the packet size is within the specified bandwidth limit.

Table 117. Other Event Logs: Bandwidth Limit, Inbound Bandwidth Profile

Message	2000 Jan 1 00:08:21 [SRX5308] [kernel] [BW_LIMIT_DROP] IN=LAN OUT=WAN SRC=22.0.0.2 DST=192.168.100.2 PROTO=ICMP TYPE=112 CODE=113 TC_INDEX=10 CLASSID=10:2
Explanation	This log is generated when an inbound packet is dropped because the packet size exceeds the specified bandwidth limit.
Recommended Action	Ensure that the packet size is within the specified bandwidth limit.

DHCP Logs

This section explains the log messages that are generated when a host is assigned a dynamic IP address. These messages are displayed on the DHCP Log screen (see *View the DHCP Log* on page 288).

Table 118. DHCP Logs

Message 1	2000 Jan 1 07:27:28 [SRX5308] [dhcpd] Listening on LPF/eth0.1/00:11:22:78:89:90/192.168.11/24
Message 2	2000 Jan 1 07:27:37 [SRX5308] [dhcpd] DHCPRELEASE of 192.168.10.2 from 00:0f:1f:8f:7c:4a via eth0.1 (not found)
Message 3	2000 Jan 1 07:27:47 [SRX5308] [dhcpd] DHCPDISCOVER from 00:0f:1f:8f:7c:4a via eth0.1
Message 4	2000 Jan 1 07:27:48 [SRX5308] [dhcpd] DHCPOFFER on 192.168.11.2 to 00:0f:1f:8f:7c:4a via eth0.1
Message 5	2000 Jan 1 07:27:48 [SRX5308] [dhcpd] Wrote 2 leases to leases file.
Message 6	2000 Jan 1 07:27:48 [SRX5308] [dhcpd] DHCPREQUEST for 192.168.11.2 (192.168.11.1) from 00:0f:1f:8f:7c:4a via eth0.1
Message 7	2000 Jan 1 07:27:48 [SRX5308] [dhcpd] DHCPACK on 192.168.11.2 to 00:0f:1f:8f:7c:4a via eth0.1

Table 118. DHCP Logs (continued)

Explanation	Message 1: The DHCP server is listening on eth0.1. Message 2: Release of the currently assigned IP address from the host by the DHCP server. Message 3: DHCP broadcast by the host is discovered by the DHCP server. Message 4: The DHCP server offers a new IP address to the host’s current network interface. Message 5: Two new leases are written to the lease file. Message 6: DHCP is requested to assign the new IP address by the host. Message 7: DHCP acknowledgment to the current network interface from the server on assignment of the new IP address.
Recommended Action	None

Two-Factor Authentication D

This appendix provides an overview of Two-Factor Authentication, and an example of how to implement the WiKID solution.

This appendix contains the following sections:

Why Do I Need Two-Factor Authentication?

In today’s market, online identity theft and online fraud continue to be one of the fast-growing cyber crime activities used by many unethical hackers and cyber criminals to steal digital assets for financial gains. Many companies and corporations are losing millions of dollars and running into risks of revealing their trade secrets and other proprietary information as the results of these cyber crime activities. Security threats and hackers have become more sophisticated, and user names, encrypted passwords, and the presence of firewalls are no longer enough to protect the networks from being compromised. IT professionals and security experts have recognized the need to go beyond the traditional authentication process by introducing and requiring additional factors to the authentication process. NETGEAR has also recognized the need to provide more than just a firewall to protect the networks. NETGEAR has implemented a more robust authentication system known as Two-Factor Authentication (2FA or T-FA) to help address the fast-growing network security issues.

What Are the Benefits of Two-Factor Authentication?

- **Stronger security.** Passwords cannot efficiently protect the corporate networks because attackers can easily guess simple passwords or users cannot remember complex and unique passwords. One-time passcode (OTP) strengthens and replaces the need to remember complex password.
- **No need to replace existing hardware**. Two-Factor Authentication can be added to existing NETGEAR products through a firmware upgrade.

- **Quick to deploy and manage**. The WiKID solution integrates seamlessly with the NETGEAR SSL and VPN firewall products.
- **Proven regulatory compliance**. Two-Factor Authentication has been used as a mandatory authentication process for many corporations and enterprises worldwide.

What Is Two-Factor Authentication

Two-factor authentication is a security solution that enhances and strengthens security by implementing multiple factors of the authentication process that challenge and confirm the users' identities before they can gain access to the network. There are several factors that are used to validate the users to make sure that you are who you said you are. These factors are:

- Something you know—for example, your password or your PIN.
- Something you have—for example, a token with generated passcode that is 6 to 8 digits in length.
- Something you are—for example, biometrics such as fingerprints or retinal prints.

This appendix focuses on and discusses only the first two factors, something you know and something you have. This security method can be viewed as a two-tiered authentication approach because it typically relies on what you know and what you have. A common example of two-factor authentication is a bank (ATM) card that has been issued by a bank institute:

- The PIN to access your account is "*something you know.*"
- The ATM card is "*something you have.*"

You need to have both of these factors to gain access to your bank account. Similar to the way ATM cards work, access to the corporate networks and data can also be strengthened using a combination of multiple factors such as a PIN and a token (hardware or software) to validate the users and reduce the incidence of online identity theft.

NETGEAR Two-Factor Authentication Solutions

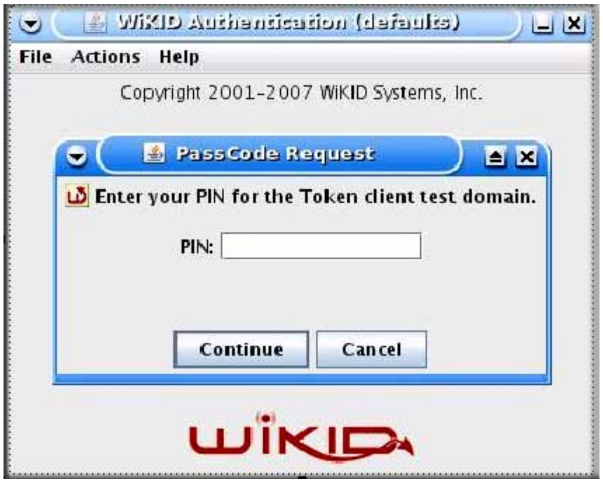
NETGEAR has implemented 2 Two-Factor Authentication solutions from WiKID. WiKID is the software-based token solution. So instead of using only Windows Active Directory or LDAP as the authentication server, administrators now have the option to use WiKID to perform Two-Factor Authentication on NETGEAR SSL and VPN firewall products.

The WiKID solution is based on a request-response architecture where a one-time passcode (OTP), which is time-synchronized with the authentication server, is generated and sent to the user after the validity of a user credential has been confirmed by the server.

The request-response architecture is capable of self-service initialization by end users, dramatically reducing implementation and maintenance costs. Here is an example of how WiKID works.

➢ To use WiKID (for end users):

1. Launch the WiKID token software, enter the PIN that has been provided (*something the user knows*), and then click **Continue** to receive the OTP from the WiKID authentication server:



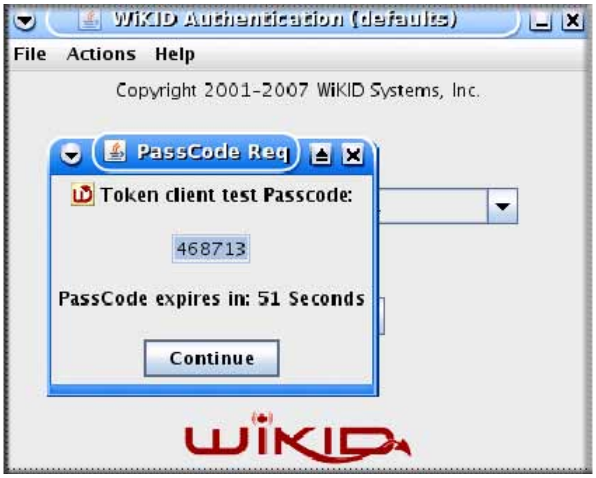
Copyright 2001-2007 WiKID Systems, Inc.

Enter your PIN for the Token client test domain.

PIN:

Figure 202.

2. A one-time passcode (*something the user has*) is generated.



Copyright 2001-2007 WiKID Systems, Inc.

Token client test Passcode:

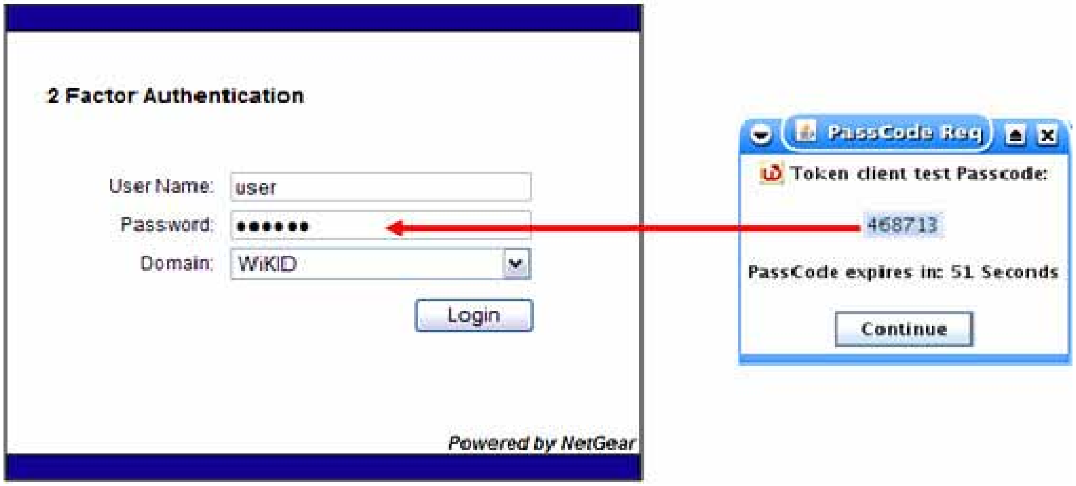
468713

PassCode expires in: 51 Seconds

Figure 203.

Note: The one-time passcode is time-synchronized to the authentication server so that the OTP can be used only once and needs to be used before the expiration time. If a user does not use this passcode before it is expired, the user needs to go through the request process again to generate a new OTP.

3. Proceed to the 2 Factor Authentication login screen and enter the one-time passcode as the login password.



2 Factor Authentication

User Name: user

Password: ••••••

Domain: WiKID

Token client test Passcode:

468713

PassCode expires in: 51 Seconds

Figure 204.

Notification of Compliance

E

NETGEAR Wired Products

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration Of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308 complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications made to the product, unless expressly approved by NETGEAR, Inc., could void the user's right to operate the equipment.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus, ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308, does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada.

European Union

The ProSafe Gigabit Quad WAN SSL VPN Firewall SRX5308 complies with essential requirements of EU EMC Directive 2004/108/EC and Low Voltage Directive 2006/95/EC as supported by applying the following test methods and standards:

- EN55022: 2006 / A1: 2007
- EN55024: 1998 / A1: 2001 / A2 : 2003
- EN60950-1: 2005 2nd Edition
- EN 61000-3-2:2006
- EN 61000-3-3:1995 w/A1: 2001+A2: 2005

GPL License Agreement

GPL may be included in this product; to view the GPL license agreement go to *ftp://downloads.netgear.com/files/GPLnotice.pdf.*

For GNU General Public License (GPL) related information, please visit *http://support.netgear.com/app/answers/detail/a_id/2649*.

Index